

# 해킹과 포렌식

김종민(dakuo)

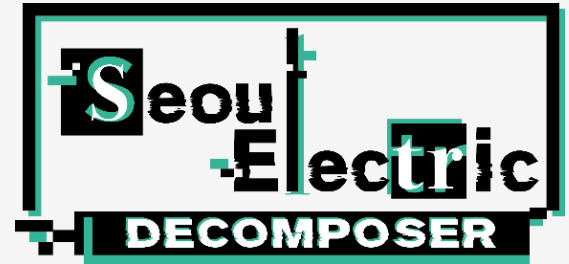
# 디지털 포렌식 멘토 – 김종민



해킹팀

Seoul Electric Decomposer 단장

<https://fb.com/SEDcmpsr>



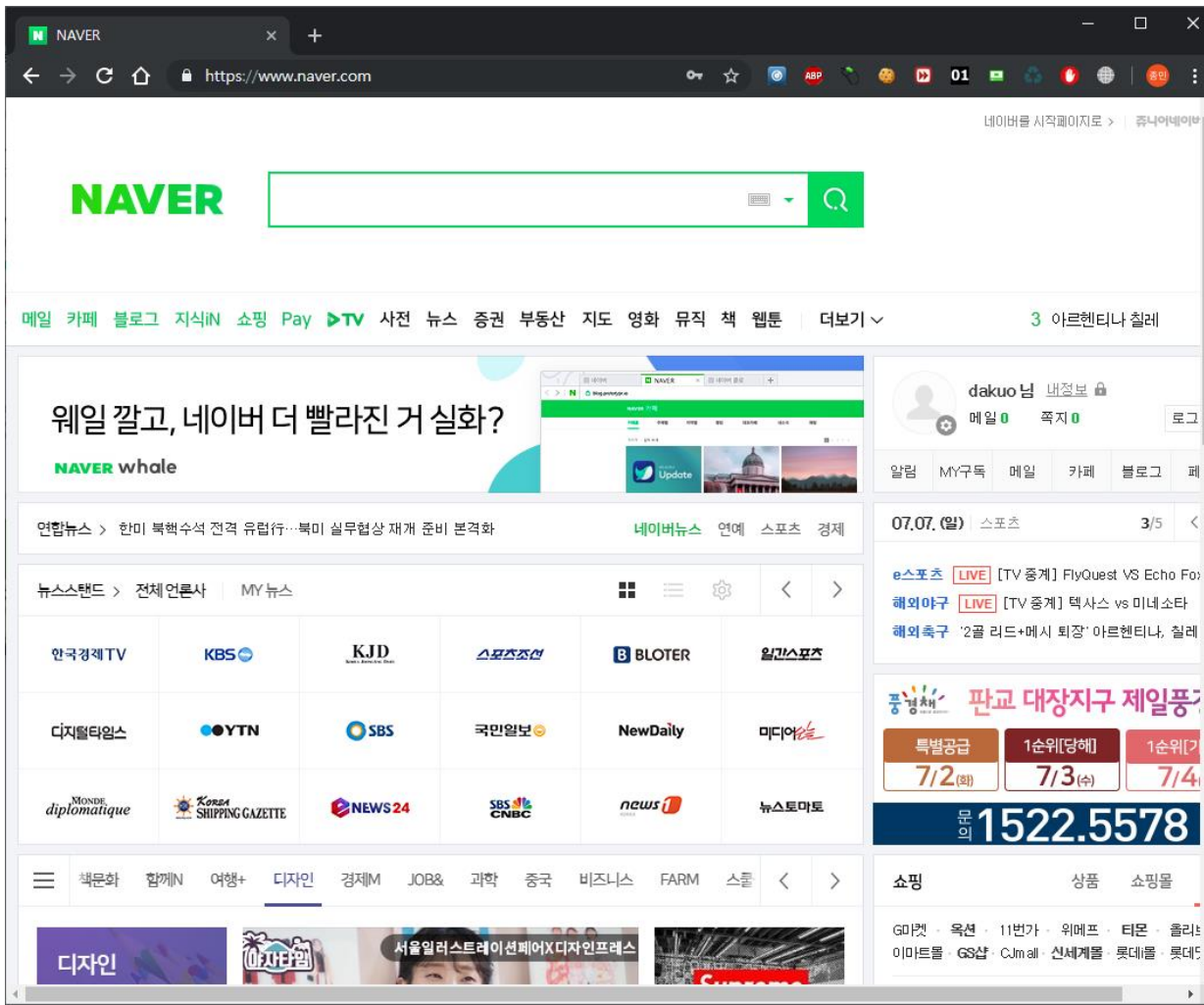
- 고려대학교 컴퓨터보안연구실 박사수료
- 차세대 보안리더(BoB) 멘토
- 소프트웨어 마에스트로 멘토
- SNS – <https://fb.com/hkdakuo>
- Phone – 010-3492-0792
- Mail – hkdakuo at gmail.com
- BoB 프로젝트 다빈치코드 팀 – 멘토
- HDCON - 2014 우승, 2015 금상
- CCE – 2017 방어 우승, 2018 방어 준우승
- DEF CON – 2014, 2017, 2018, 2019 본선
- BoB 1기 최종 6인
- 다수 강의, 프로젝트 수행

# 해킹과 포렌식

1. 웹 공격
2. 시스템 공격
3. 추가

# 1. 웹 공격

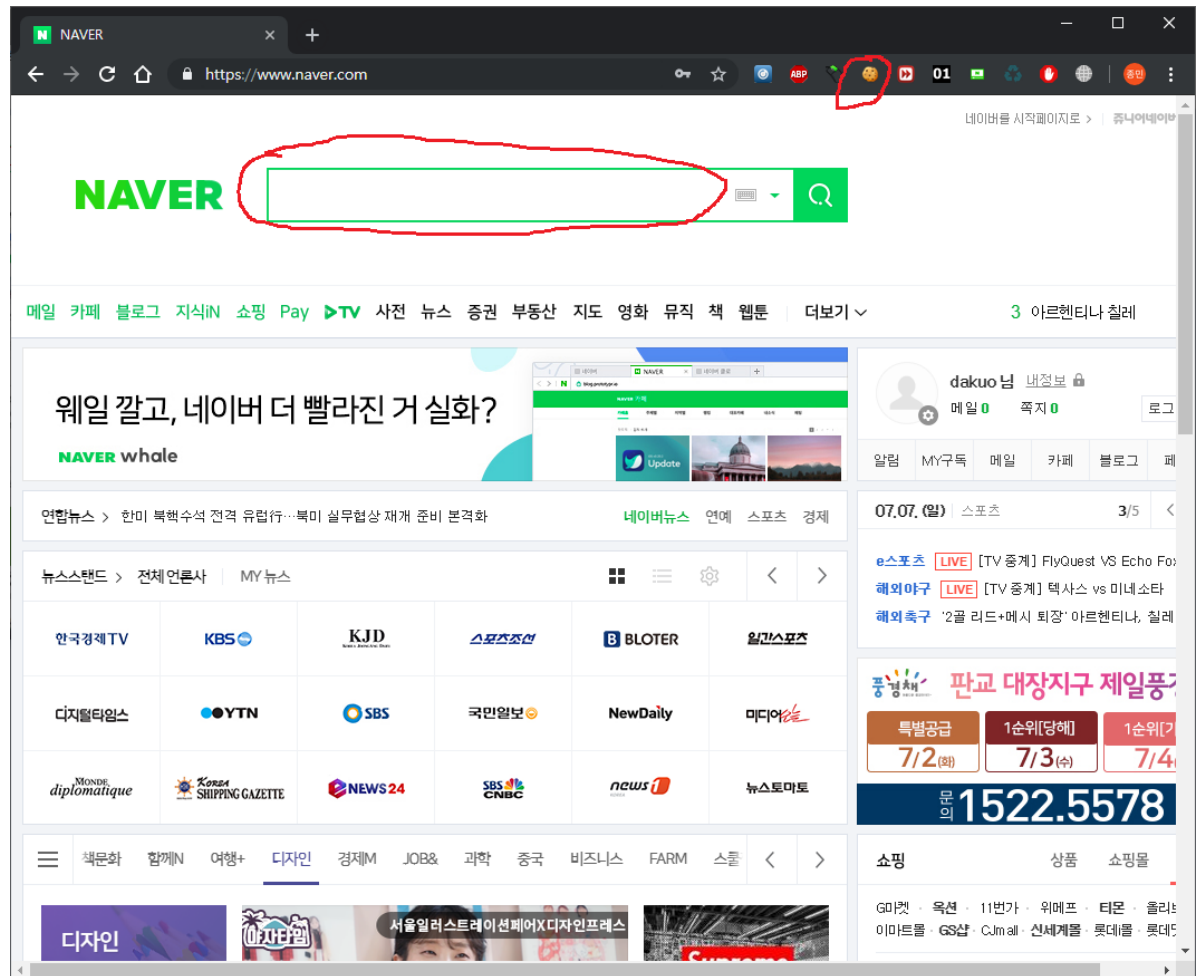
- WEB Attack Vector



# 1. 웹 공격

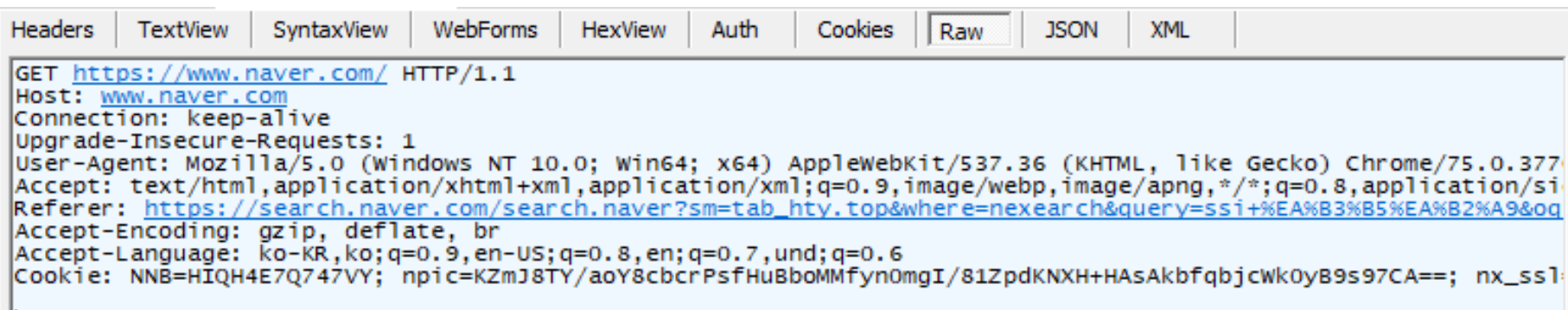
- WEB Attack Vector

- XSS
- CSRF
- SQLI
- File Upload
- ...



# 1. 웹 공격

- WEB Attack Payload



The image shows a screenshot of a web browser's developer tools, specifically the 'Raw' tab under the 'Headers' section. It displays the raw HTTP request for a GET request to <https://www.naver.com/>. The request includes standard headers such as Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept, Referer, Accept-Encoding, Accept-Language, and a Cookie.

```
GET https://www.naver.com/ HTTP/1.1
Host: www.naver.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.377
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/si
Referer: https://search.naver.com/search.naver?sm=tab_hyt.top&where=nexearch&query=ssi+%EA%B3%B5%EA%B2%A9&oq
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7,und;q=0.6
Cookie: NNB=HIQH4E7Q747VY; npic=KZmJ8TY/aoY8cbcrPsfHuBboMMfyn0mgI/81ZpdKNXH+HAsAkbfqbjcwk0yB9s97CA==; nx_ssl
```

# 1. 웹 공격

- 웹 서버
  - 서버 사이드 스크립트
  - 웹 서버 데몬
  - 커널
  - 네트워크 드라이버
  - 랜 카드



# 1. 웹 공격

- OSI 7계층





# 1. 웹 공격

- 웹 공격 과정



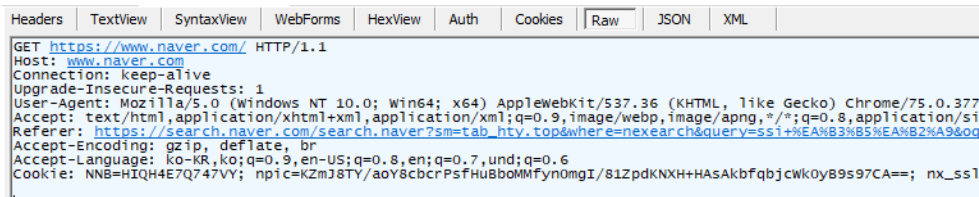
해커



웹 서버

# 1. 웹 공격

- 웹 공격 과정 1



Headers   TextView   SyntaxView   WebForms   HexView   Auth   Cookies   Raw   JSON   XML

```
GET https://www.naver.com/ HTTP/1.1
Host: www.naver.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.377
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/si
Referer: https://search.naver.com/search.naver?sm=tab_hvy.top&where=nexear ch&query=ss1+%E%83%B5%E%82%A9&oq
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR, ko;q=0.9, en-US;q=0.8, en;q=0.7, und;q=0.6
Cookie: NNB=HIQH4E7Q747VY; npic=KZm38TY/aoY8cbcrPsfHu8boMMFyn0mgI/81ZpdKNXH+HasAkbfqbjcwk0yB9s97CA==; nx_ss1
```



해커



웹 서버

# 1. 웹 공격

- 웹 공격 과정 2



# 1. 웹 공격

## • 웹 공격 과정 3

- 웹 서버
  - 서버 사이드 스크립트
  - 웹 서버 데몬
  - 커널
  - 네트워크 드라이버
  - 랜 카드



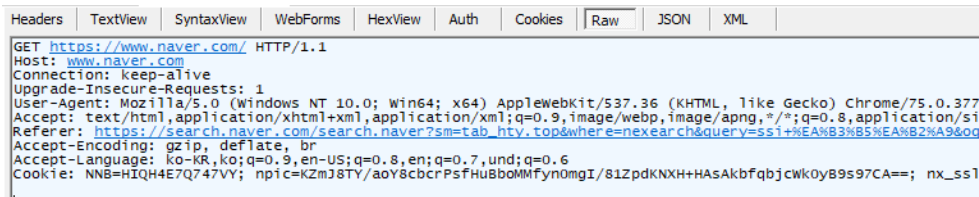
해커



웹 서버

# 1. 웹 공격

- 웹 공격 과정 1



Headers   TextView   SyntaxView   WebForms   HexView   Auth   Cookies   Raw   JSON   XML

```
GET https://www.naver.com/ HTTP/1.1
Host: www.naver.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.377
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/si
Referer: https://search.naver.com/search.naver?sm=tab_hvy.top&where=nexear ch&query=ss1+%EA%B3%B5%EA%B2%A9&oq
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR, ko;q=0.9, en-US;q=0.8, en;q=0.7, und;q=0.6
Cookie: NNB=HIQH4E7Q747VY; npic=KZm38TY/aoY8cbcrPsfHu8boMMFyn0mgI/81ZpdKNXH+HasAkbfqbjcwk0yB9s97CA==; nx_ss1
```



해커



웹 서버

# 1. 웹 공격

- 웹 공격 과정 1

```
Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML
GET https://www.naver.com/ HTTP/1.1
Host: www.naver.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.377
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/si
Referer: https://search.naver.com/search.naver?sm=tab_hvy_top&where=nexear ch&query=ss1+%EA%B3%B5%EA%B2%A9&oq
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR, ko;q=0.9, en-US;q=0.8, en;q=0.7, und;q=0.6
Cookie: NNB=HIQH4E7Q747VY; npic=KZm38TY/aoY8cbcrPsfHu8boMMfyn0mgI/81ZpdKNXH+HasAkbfqbjcWk0yB9s97CA==; nx_ss1
```



해커



웹 서버

해커 컴퓨터를 압수하지 않는 이상 분석 불가

만약, 압수 할 수 있다면?

# 1. 웹 공격

## • 웹 공격 과정 1

```
Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML
GET https://www.naver.com/ HTTP/1.1
Host: www.naver.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.377
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/si
Referer: https://search.naver.com/search.naver?sm=tab_hvy_top&where=nexearch&query=ss1+%EA%B3%B5%EA%B2%A9&q
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR, ko;q=0.9, en-US;q=0.8, en;q=0.7, und;q=0.6
Cookie: NNB=HIQH4E7Q747VY; np1c=KZm38TY/aoY8cbcrPsfHu8boMMfyn0mgI/81ZpdKNXH+HasAkbfqbjcWk0yB9s97CA==; nx_ss1
```



해커



웹 서버

1. 웹 브라우저를 통해서 접속
  - 웹 브라우저 로그 확인(시크릿 모드 사용시 할 거 없음)
2. 피들러 등 도구 사용
  - 도구 기록 확인(저장 안 했으면 할 거 없음)
3. 직접 작성한 스크립트 사용
  - 소스와 유저가 남긴 로그가 남아있지 않으면, 할 거 없음

# 1. 웹 공격

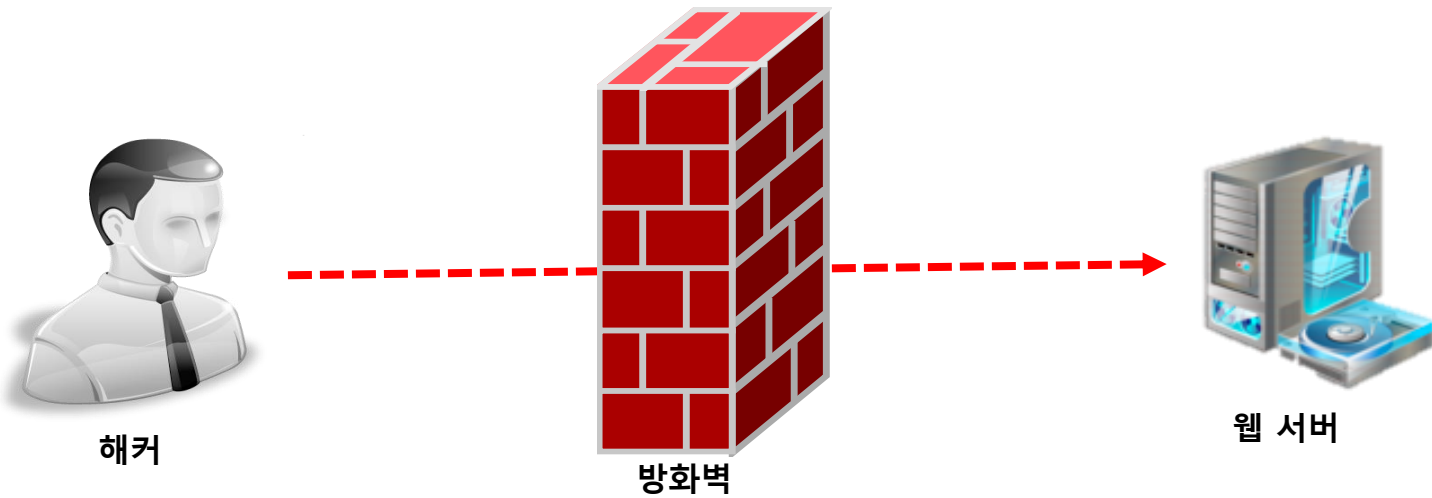
- 웹 공격 과정 2





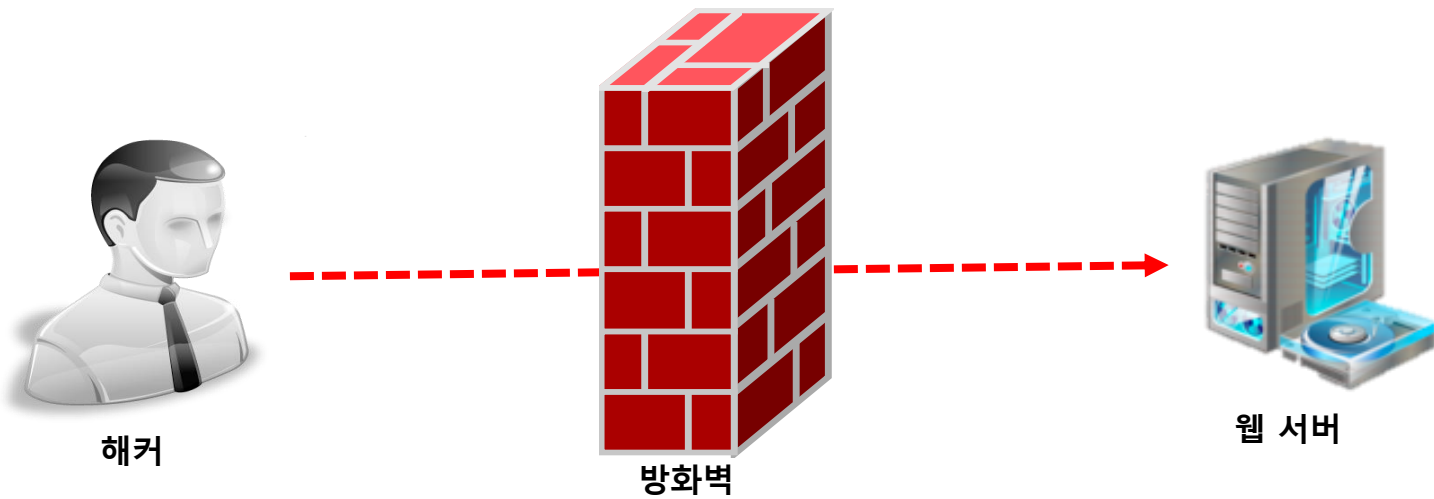
# 1. 웹 공격

- 웹 공격 과정 2



# 1. 웹 공격

- 웹 공격 과정 2

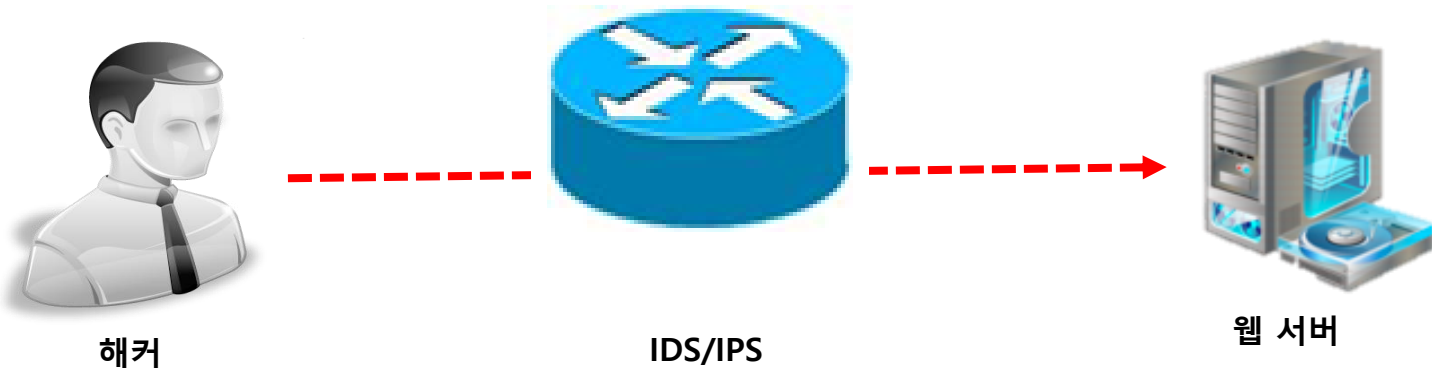


1. 방화벽 (L4)

- 해커의 IP와 PORT만 확인 가능

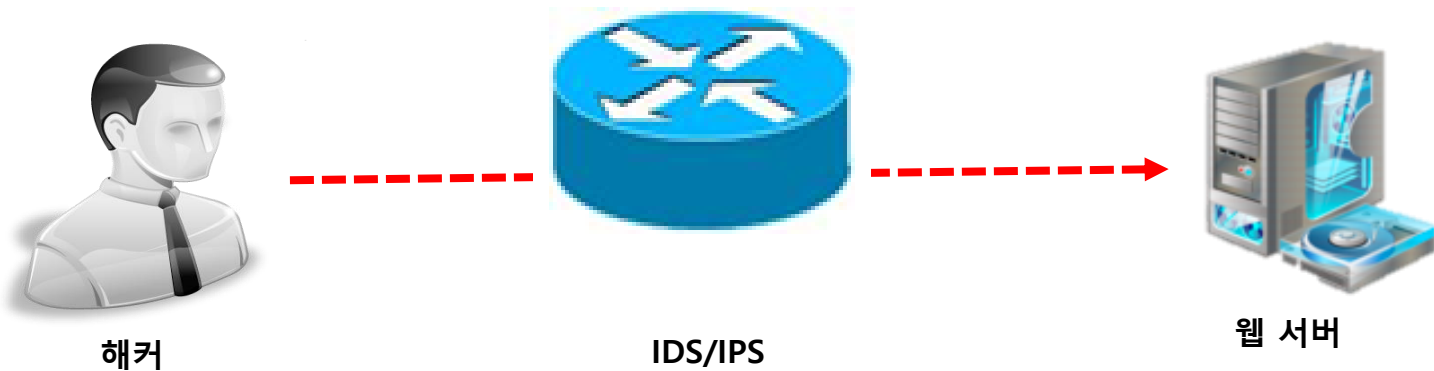
# 1. 웹 공격

- 웹 공격 과정 2



# 1. 웹 공격

- 웹 공격 과정 2

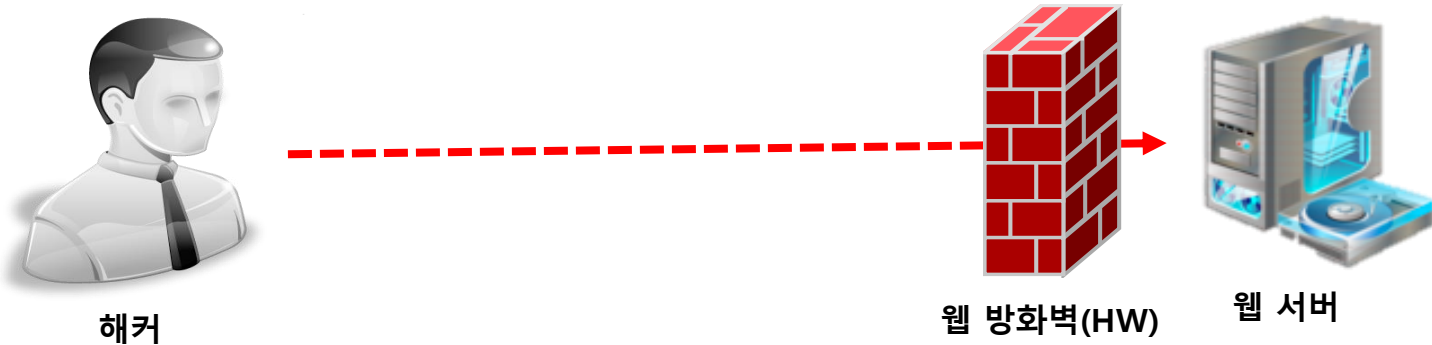


1. IDS/IPS (L4 이상)

- TCP/IP에서의 패킷 데이터 확인 가능

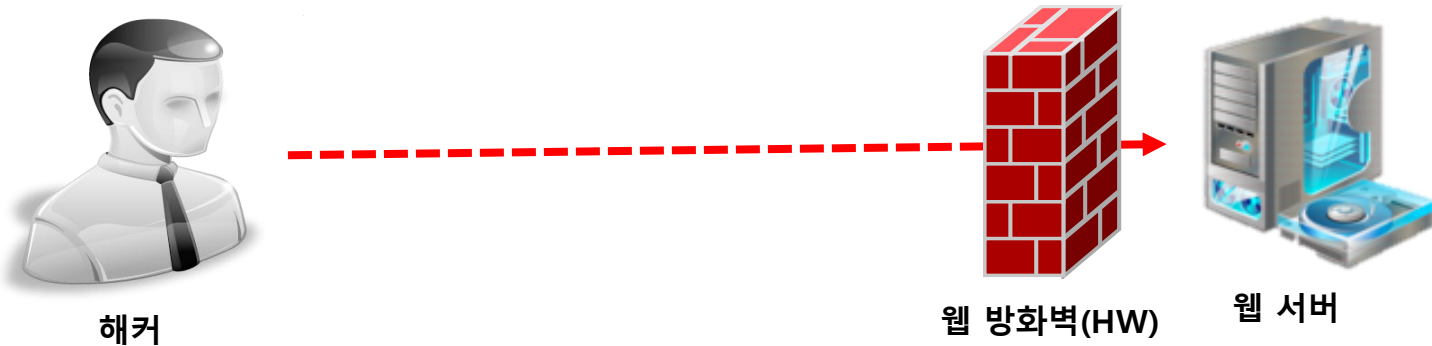
# 1. 웹 공격

- 웹 공격 과정 2



# 1. 웹 공격

- 웹 공격 과정 2



1. WAF (Web Application Firewall) (L7)
  - HTTP 데이터 확인 가능

# 1. 웹 공격

- 웹 공격 과정 3

- 웹 서버
  - 서버 사이드 스크립트
  - 웹 서버 데몬
  - 커널
  - 네트워크 드라이버
  - 랜 카드



해커



웹 서버

# 1. 웹 공격

- 웹 공격 과정 3

- 웹 서버

- 랜 카드



해커



웹 서버



# 1. 웹 공격

- 웹 공격 과정 3

- 웹 서버



해커



- 랜 카드



웹 서버

모름...

# 1. 웹 공격

- 웹 공격 과정 3

- 웹 서버



해커



- 네트워크 드라이버
- 랜 카드



웹 서버

# 1. 웹 공격

- 웹 공격 과정 3

- 웹 서버



해커



- 네트워크 드라이버
- 랜 카드



웹 서버

패킷 데이터 덤프하는 기능이  
활성화 되어있지 않으면 아무것도 없음

# 1. 웹 공격

- 웹 공격 과정 3

- 웹 서버

- 커널
- 네트워크 드라이버
- 랜 카드



해커



웹 서버

# 1. 웹 공격

- 웹 공격 과정 3

- 웹 서버

- 커널
- 네트워크 드라이버
- 랜 카드



해커



웹 서버

1. Iptables log 활성화 시(/var/log/messages)
2. Syslog

# 1. 웹 공격

- 웹 공격 과정 3

- 웹 서버

- 웹 서버 데몬
- 커널
- 네트워크 드라이버
- 랜 카드



해커



웹 서버

# 1. 웹 공격

## • 웹 공격 과정 3



해커

## • 웹 서버

- 웹 서버 데몬
- 커널
- 네트워크 드라이버
- 랜 카드



웹 서버

1. 웹 방화벽(SW) 설치 후 가동
2. 웹 서버 데몬 모듈 가동
3. 웹 서버 데몬 로그 (/var/log/access.log)

```
1/Oct/2015:15:45:09 +0200] "GET / HTTP/1.1" 200 4797 "-" "Pingdom.com_
0ct/2015:15:46:10 +0200] "GET / HTTP/1.1" 200 4797 "-" "Pingdom.com_bo
[11/Oct/2015:15:47:09 +0200] "GET / HTTP/1.1" 200 4797 "-" "Pingdom.com_
1/Oct/2015:15:48:09 +0200] "GET / HTTP/1.1" 200 4797 "-" "Pingdom.com_bo
11/Oct/2015:15:49:09 +0200] "GET / HTTP/1.1" 200 4797 "-" "Pingdom.com_bo
1/Oct/2015:15:50:06 +0200] "POST /autodiscover/autodiscover.xml HTTP/1.1"
11/Oct/2015:15:50:09 +0200] "GET / HTTP/1.1" 200 4797 "-" "Pingdom.com_bo
1/Oct/2015:15:50:22 +0200] "POST /autodiscover/autodiscover.xml HTTP/1.1"
1/Oct/2015:15:51:09 +0200] "GET / HTTP/1.1" 200 4797 "-" "Pingdom.com_bot_v
```

# 1. 웹 공격

- 웹 공격 과정 3

- 웹 서버
  - 서버 사이드 스크립트
  - 웹 서버 데몬
  - 커널
  - 네트워크 드라이버
  - 랜 카드



해커



웹 서버



# 1. 웹 공격

## • 웹 공격 과정 3

### • 웹 서버

- 서버 사이드 스크립트
- 웹 서버 데몬
- 커널
- 네트워크 드라이버
- 랜 카드

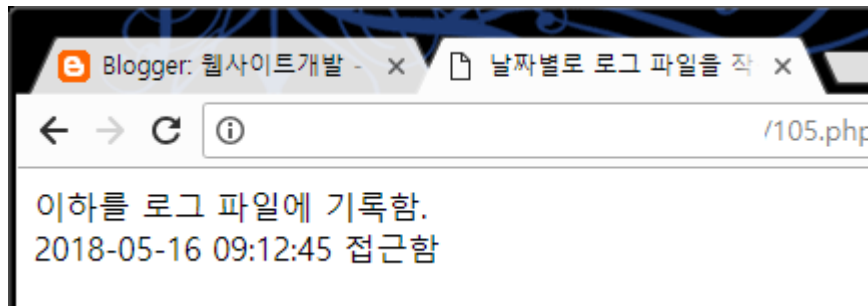


해커



웹 서버

개발자가 알아서 남김



# 1. 웹 공격

- 추가 공격
  - 웹 사이트 변조
  - 프로그램 실행
  - 파일 생성
  - 권한 획득

# 1. 웹 공격

- 추가 공격

- 웹 사이트 변조 ➔ 파일 로그 분석
- 프로그램 실행 ➔ 명령어 실행 기록 분석, 프로세스 분석
- 파일 생성 ➔ 파일 로그 분석
- 권한 획득 ➔ 명령어 실행 기록 분석

# 1. 웹 공격

- 추가 공격

- 웹 사이트 변조 → 파일 로그 분석, DB 로그 분석
- 프로그램 실행 → 명령어 실행 기록 분석, 프로세스 분석
- 파일 생성 → 파일 로그 분석
- 권한 획득 → 명령어 실행 기록 분석

OS(+정책), 파일 시스템, 어플리케이션에  
의존적(Dependency)

## 2. 시스템 공격

- 프로그램(데몬)을 공격(커널 포함)
  - Crash
  - EoP(Elevation of Privilege)
  - RCE(Remote Code Execution)

## 2. 시스템 공격

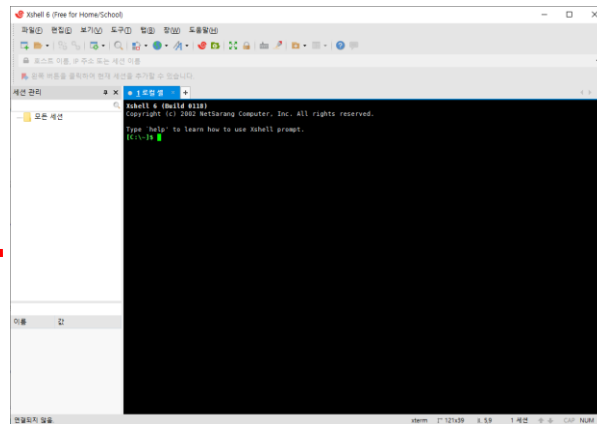
- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달
    - 이메일로 전달
    - 메신저로 전달
    - 웹 사이트 변조를 통해서 전달
    - 워터링 홀
  - 직접
    - 선물
    - 택배
    - 땅바닥에 뿌림
    - 협박
    - 원격 접속
    - 로컬 접속

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달



해커



서버

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달





## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달
- 서버
  - 프로그램
  - 서비스 데몬
  - 커널
  - 네트워크 드라이버
  - 랜 카드



해커



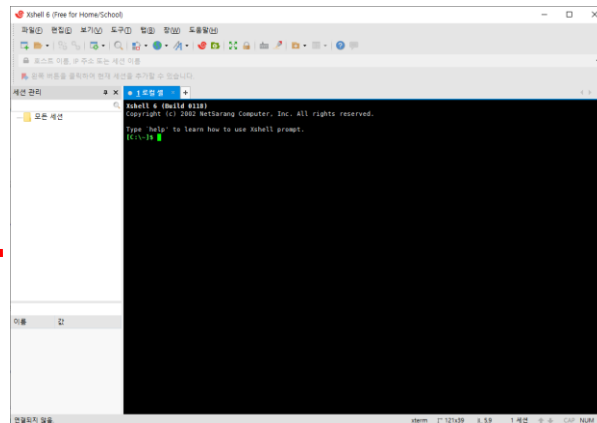
서버

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달



해커



서버

해커 컴퓨터를 압수하지 않는 이상 분석 불가

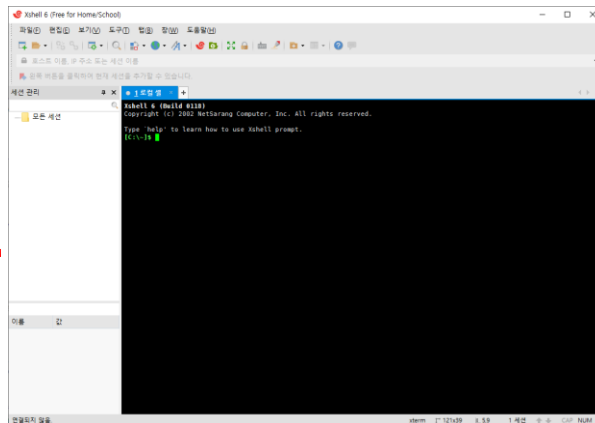
만약, 압수 할 수 있다면?

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달



해커



서버

1. 프로그램을 통해서 접속
  - 프로그램 로그 확인(프로그램 로그 없으면, 할 거 없음)
2. 직접 작성한 스크립트 사용
  - 소스와 유저가 남긴 로그가 남아있지 않으면, 할 거 없음
3. 디스크 검색
  - 익스플로잇을 지웠거나, 머리 속에 있으면, 할거 없음...

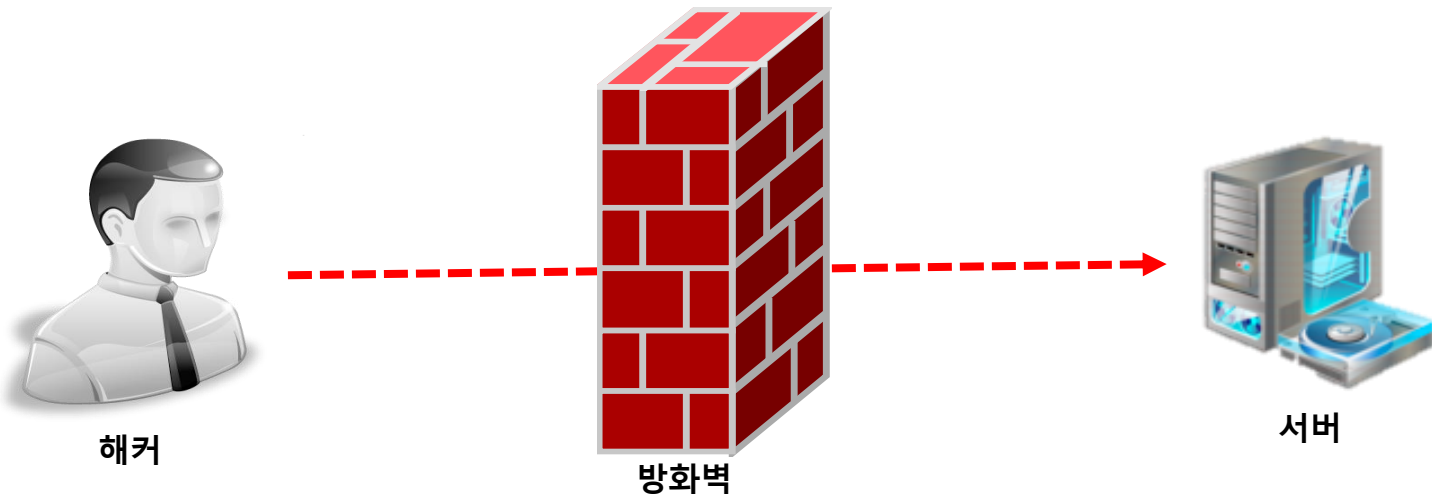
## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달



## 2. 시스템 공격

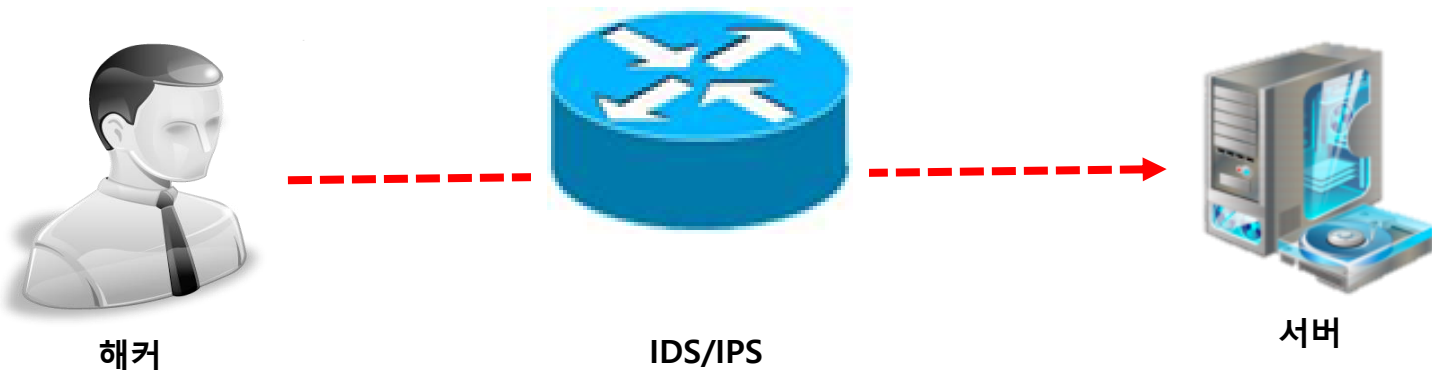
- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달



1. 방화벽 (L4)
  - 해커의 IP와 PORT만 확인 가능

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달



1. IDS/IPS (L4 이상)
  - TCP/IP에서의 패킷 데이터 확인 가능

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달
- 서버
  - 프로그램
  - 서비스 데몬
  - 커널
  - 네트워크 드라이버
  - 랜 카드



해커



서버

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달
  - 서버



해커



- 랜 카드



서버

모름...



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 서버
    - 네트워크
      - 서버의 서비스 데몬에 전달

- 네트워크 드라이버
- 랜 카드



해커



서버

패킷 데이터 덤프하는 기능이  
활성화 되어있지 않으면 아무것도 없음

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달
  - 서버

- 커널
- 네트워크 드라이버
- 랜 카드



해커



서버

1. Iptables log 활성화 시(/var/log/messages)
2. Syslog
3. Crash log

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달
- 서버
  - 서비스 데몬
  - 커널
  - 네트워크 드라이버
  - 랜 카드



해커



서버

1. 서비스 데몬 모듈 가동
2. 서비스 데몬 로그 (/var/log/XXX.log)

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달
- 서버
  - 프로그램
  - 서비스 데몬
  - 커널
  - 네트워크 드라이버
  - 랜 카드



해커



서버

개발자가 알아서 남김(예외처리)

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일로 전달



해커



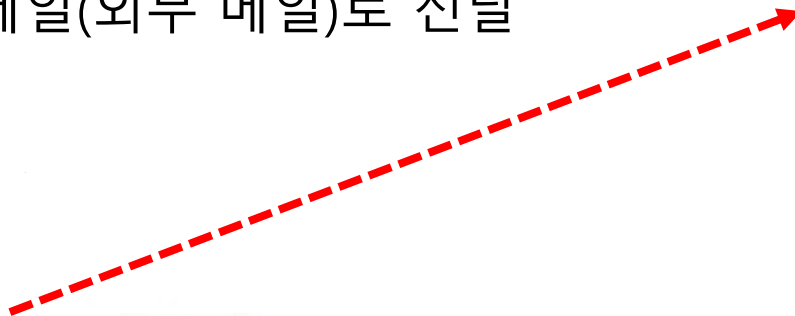
PC

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(외부 메일)로 전달



해커



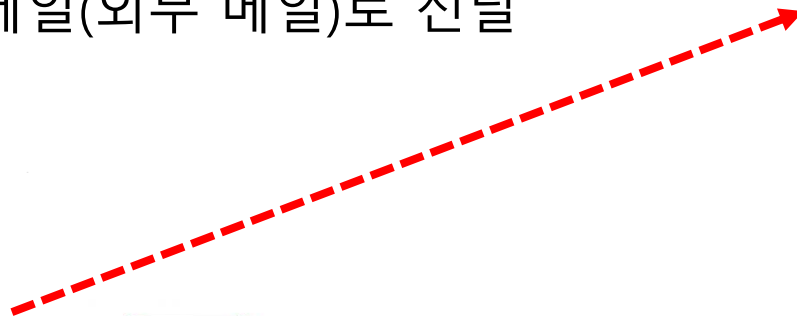
PC

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(외부 메일)로 전달



해커



PC

해커 컴퓨터를 압수할 수 없으면?

메일 계정 추적 가능  
(익명이거나 차명이면 노답)

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(외부 메일)로 전달



해커



PC

해커 컴퓨터를 압수할 수 있으면?

- 메일 보낸 흔적 포렌식
1. 웹 브라우저 로그 분석
  2. 메일 프로그램 로그 분석



## 2. 시스템 공격

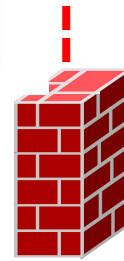
- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(외부 메일)로 전달



해커



방화벽



PC

## 2. 시스템 공격

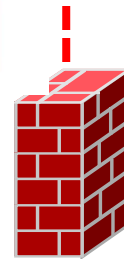
- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(외부 메일)로 전달



해커



방화벽



PC

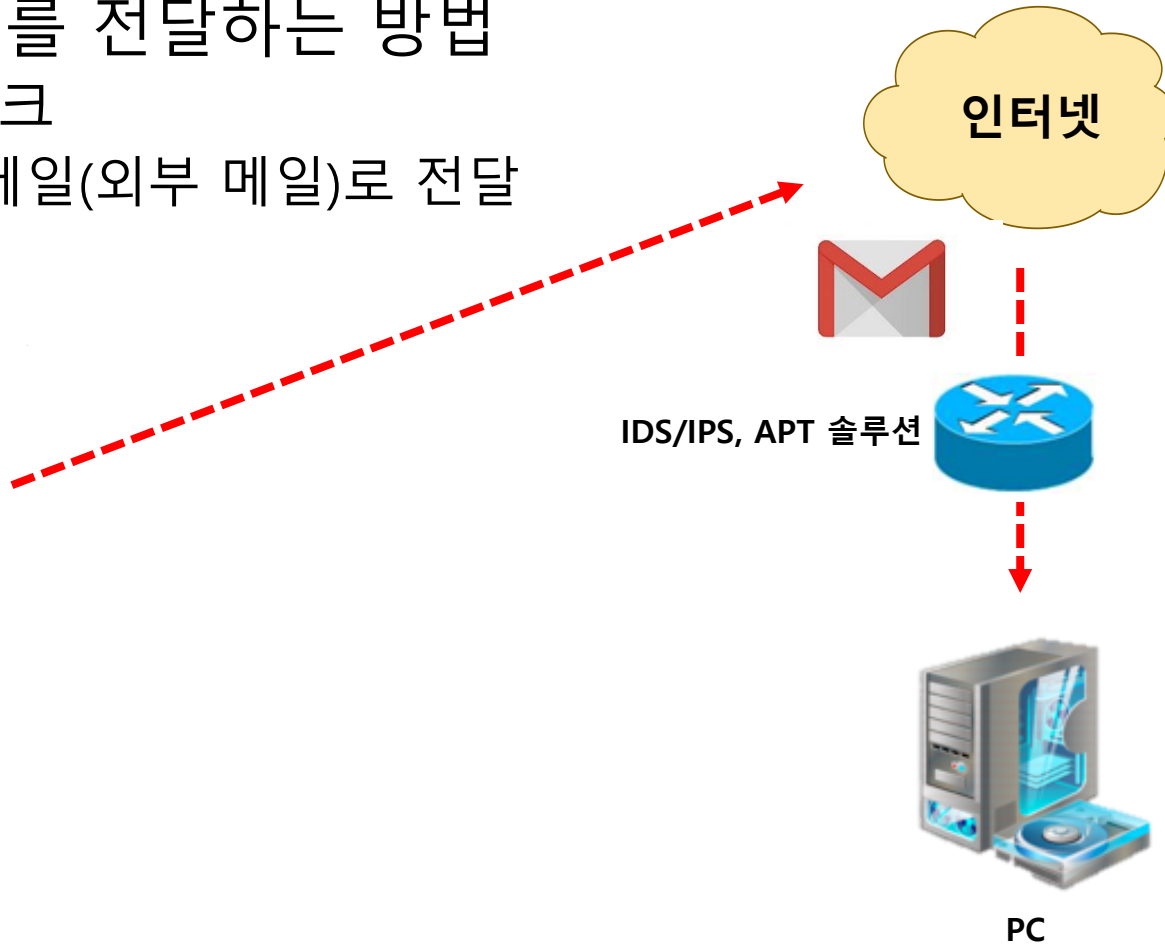
의미 없음

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(외부 메일)로 전달



해커



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(외부 메일)로 전달



해커

### 1. IDS/IPS (L4 이상)

- TCP/IP에서의 패킷 데이터 확인 가능
- HTTP 파일 다운로드 데이터 확인



IDS/IPS, APT 솔루션



PC

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(외부 메일)로 전달



해커



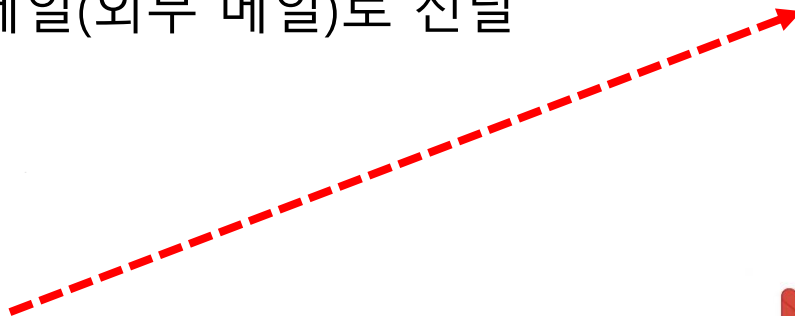
PC

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(외부 메일)로 전달



해커



PC

- 메일 받은 흔적 포렌식
1. 웹 브라우저 로그 분석
  2. 메일 프로그램 로그 분석
  3. 첨부 파일 실행 흔적 분석

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(회사 메일)로 전달



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(회사 메일)로 전달



해커 컴퓨터를 압수할 수 없으면?

메일 계정 추적 가능  
(익명이거나 차명이면 노답)



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(회사 메일)로 전달



해커 컴퓨터를 압수할 수 있으면?

메일 보낸 흔적 포렌식

1. 웹 브라우저 로그 분석
2. 메일 프로그램 로그 분석
3. 첨부 파일 검색 및 복구

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(회사 메일)로 전달



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(회사 메일)로 전달



해커가 자기 소유의 메일 서버를 이용해서  
보내지 않는 이상 의미 없음

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(회사 메일)로 전달



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(회사 메일)로 전달



### 1. IDS/IPS (L4 이상)

- TCP/IP에서의 패킷 데이터 확인 가능
- SMTP 프로토콜에서 데이터 확인

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(회사 메일)로 전달



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 이메일(회사 메일)로 전달



- 메일 받은 흔적 포렌식
1. 웹 브라우저 로그 분석
  2. 메일 프로그램 로그 분석
  3. 첨부 파일 실행 흔적 분석

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 메신저로 전달





## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 메신저로 전달



해커 컴퓨터를 압수할 수 없으면?

카카오톡 계정 추적 가능

1. 카카오톡에 협조 요청
2. 안해주면 영장
3. 영장 안해주면... 노답

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 메신저로 전달

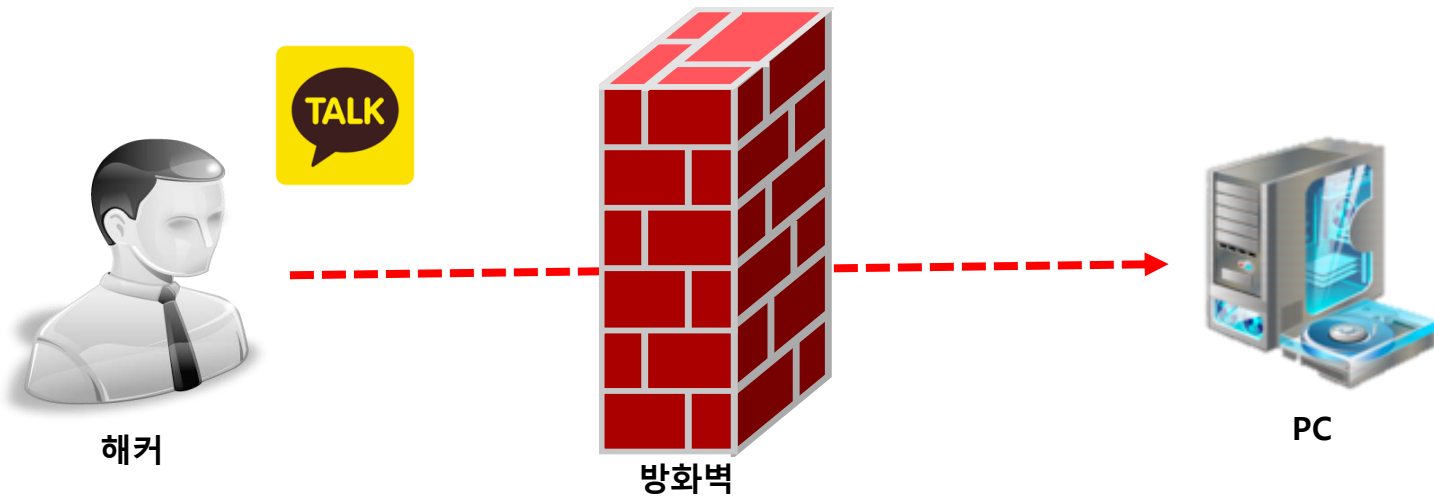


해커 컴퓨터를 압수할 수 있으면?

- 메신저 사용 내역 포렌식
1. 메신저 대화기록 복원
  2. 전송 파일 검색 및 복구

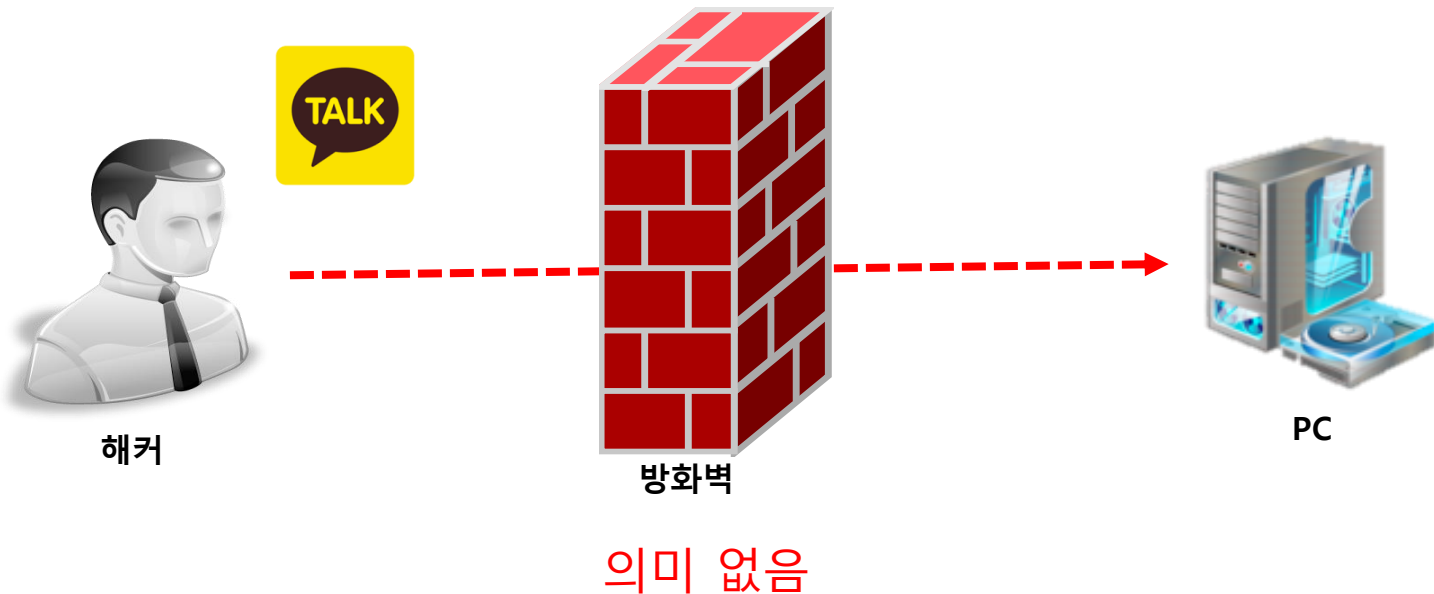
## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 메신저로 전달



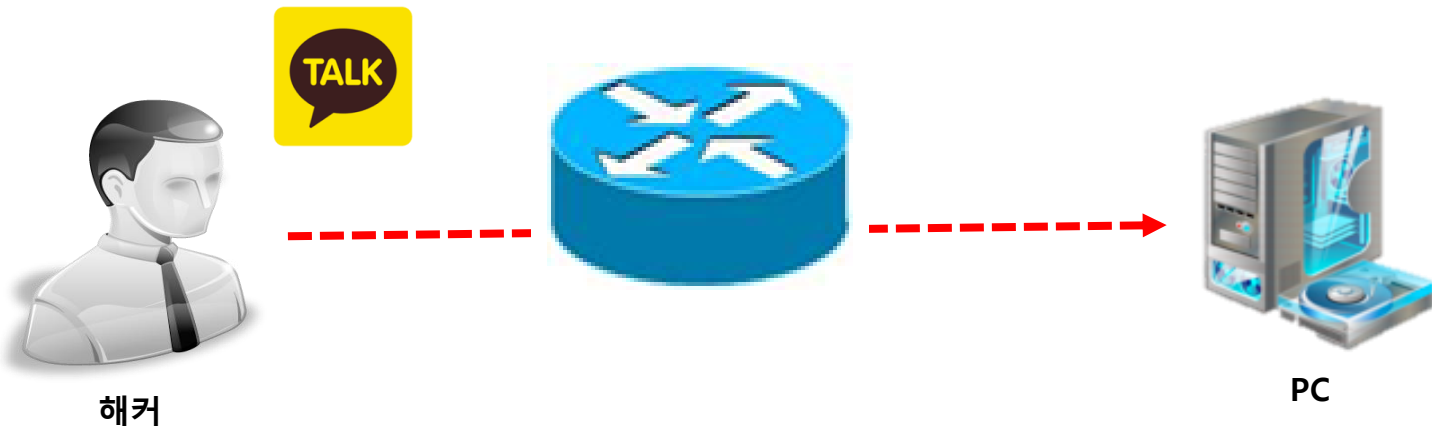
## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 메신저로 전달



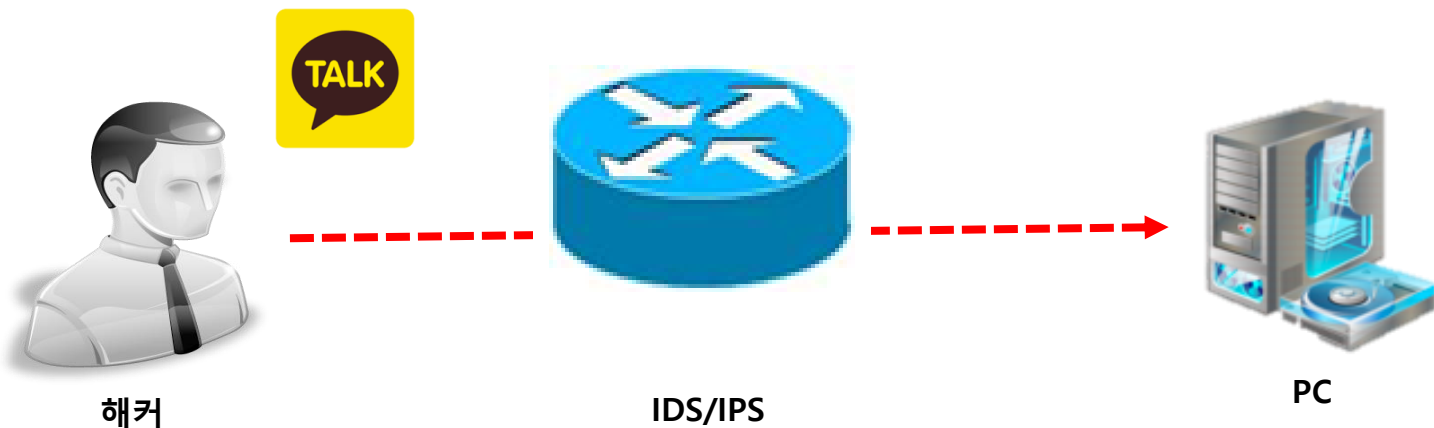
## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 메신저로 전달



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 메신저로 전달



의미 없음

의미 있으면...  
대화 내용 도청으로 회사 때려 쳐야 함

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 메신저로 전달



해커



PC

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 메신저로 전달



해커



PC

- 메신저 사용 내역 포렌식
1. 메신저 대화기록 검색 및 복원
  2. 전송 파일 검색 및 복구



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달
    - 이메일로 전달
    - 메신저로 전달
    - 웹 사이트 변조를 통해서 전달
    - 워터링 홀

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 네트워크
    - 서버의 서비스 데몬에 전달
    - 이메일로 전달
    - 메신저로 전달
      - 파일 전송 가능한 프로그램을 통한 전달과 비슷
    - 웹 사이트 변조를 통해서 전달
      - ➔ 이메일 외부 메일과 비슷 ➔ 웹 다운로드 분석
  - 워터링 홀
    - 웹 다운로드 분석
    - 파일 전송 가능한 프로그램 분석

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 직접
    - 선물
    - 택배
    - 땅바닥에 뿌림
    - 협박
    - 원격 접속
    - 로컬 접속

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 직접
    - 선물 ➔ 준 사람 조사
    - 택배 ➔ 송신자 조사
    - 외부 저장 매체 땅바닥에 뿌림 ➔ CCTV 조사
    - 협박 ➔ 협박 매체 조사
    - 원격 접속 ➔ 원격 접속 IP 조서
    - 로컬 접속
      - 옆 사람 의심
      - 사이 안 좋은 사람 의심
      - 스파이
      - 배신자
      - 몽유병
      - 내가 범인

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 직접
    - 외장 저장 매체
      - USB
      - 외장 하드
      - CD
      - 플로피 디스켓...
      - 기타

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 직접
    - 외장 저장 매체



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 직접
    - 외장 저장 매체



해커

외장  
저장  
매체



PC



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 직접
    - 외장 저장 매체



해커

정면



PC

### 출입절차

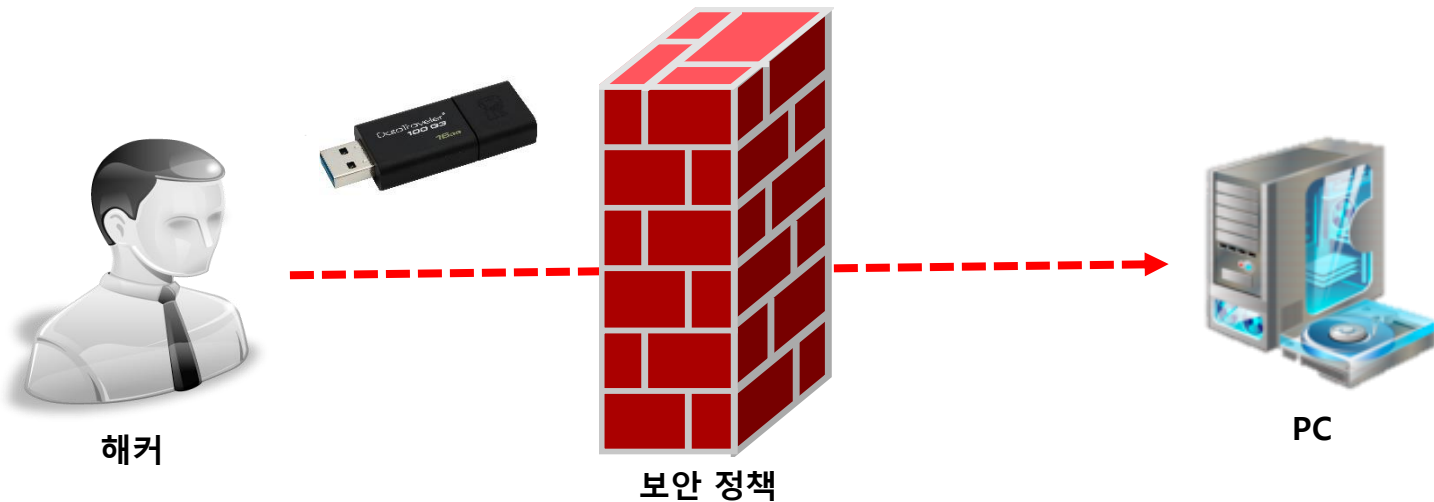
1. 사전 방문 예약
2. 담당자 대동
3. 방문 정보 기록
4. 신분증 제출
5. 전자기기 검열(사전 신고 물품만 가능)
6. 카메라 봉인 스티커





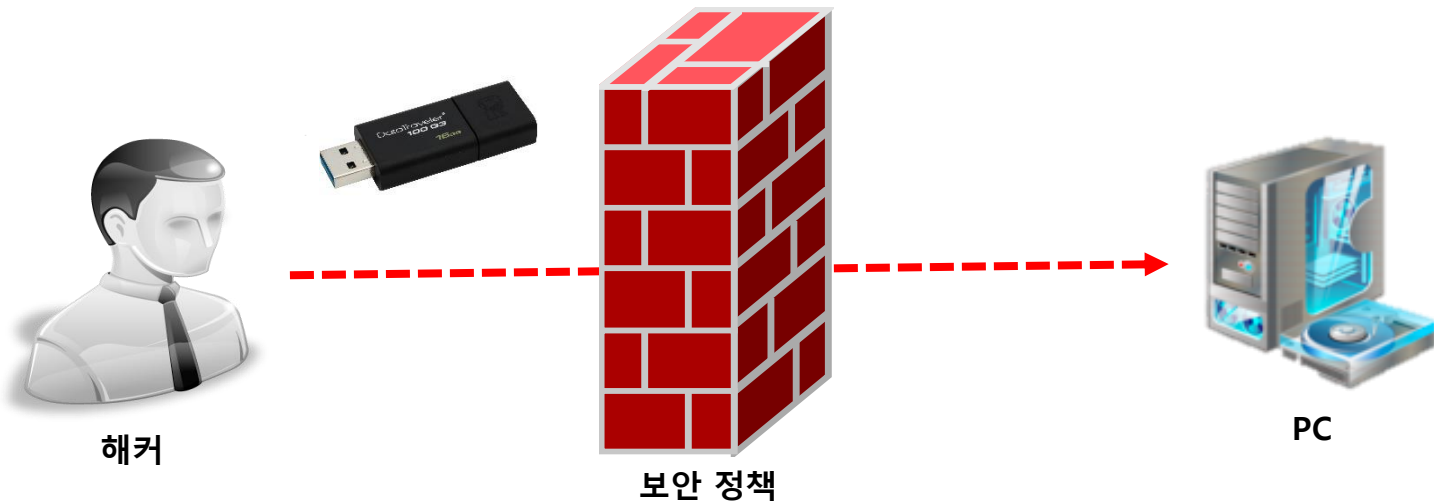
## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 직접
    - 외장 저장 매체



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 직접
    - 외장 저장 매체



1. USB 사용 금지
2. 외장 하드 사용 금지
3. 기타

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 직접
    - 외장 저장 매체



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 직접
    - 외장 저장 매체



## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 직접
    - 외장 저장 매체



해커



PC

## 2. 시스템 공격

- 공격 코드를 전달하는 방법
  - 직접
    - 외장 저장 매체



해커



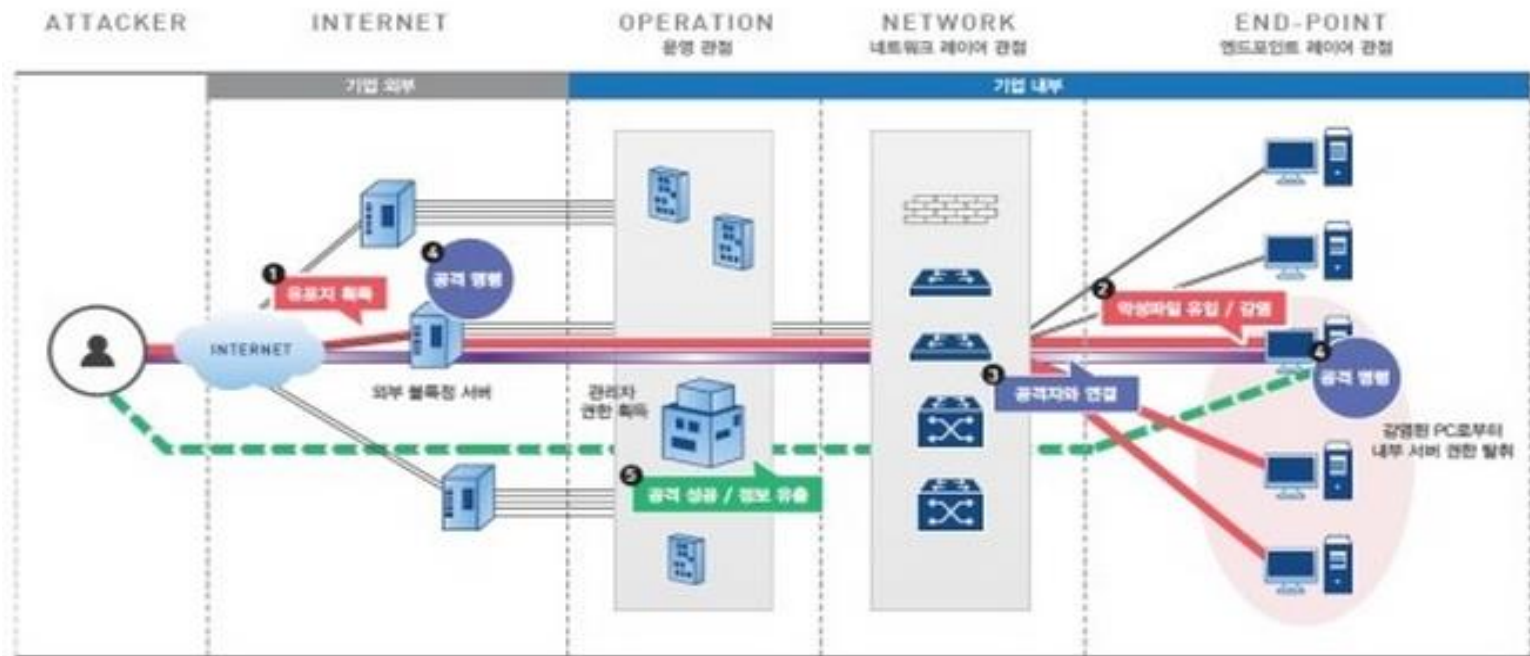
PC

- Windows
  - 레지스트리
  - Event Log
- Linux
  - Syslog

### 3. 추가

- 리얼 월드 적용

# APT Attack 다양한 프로세스



(APT 공격 진행 프로세스 : 출처 안철수 연구소)



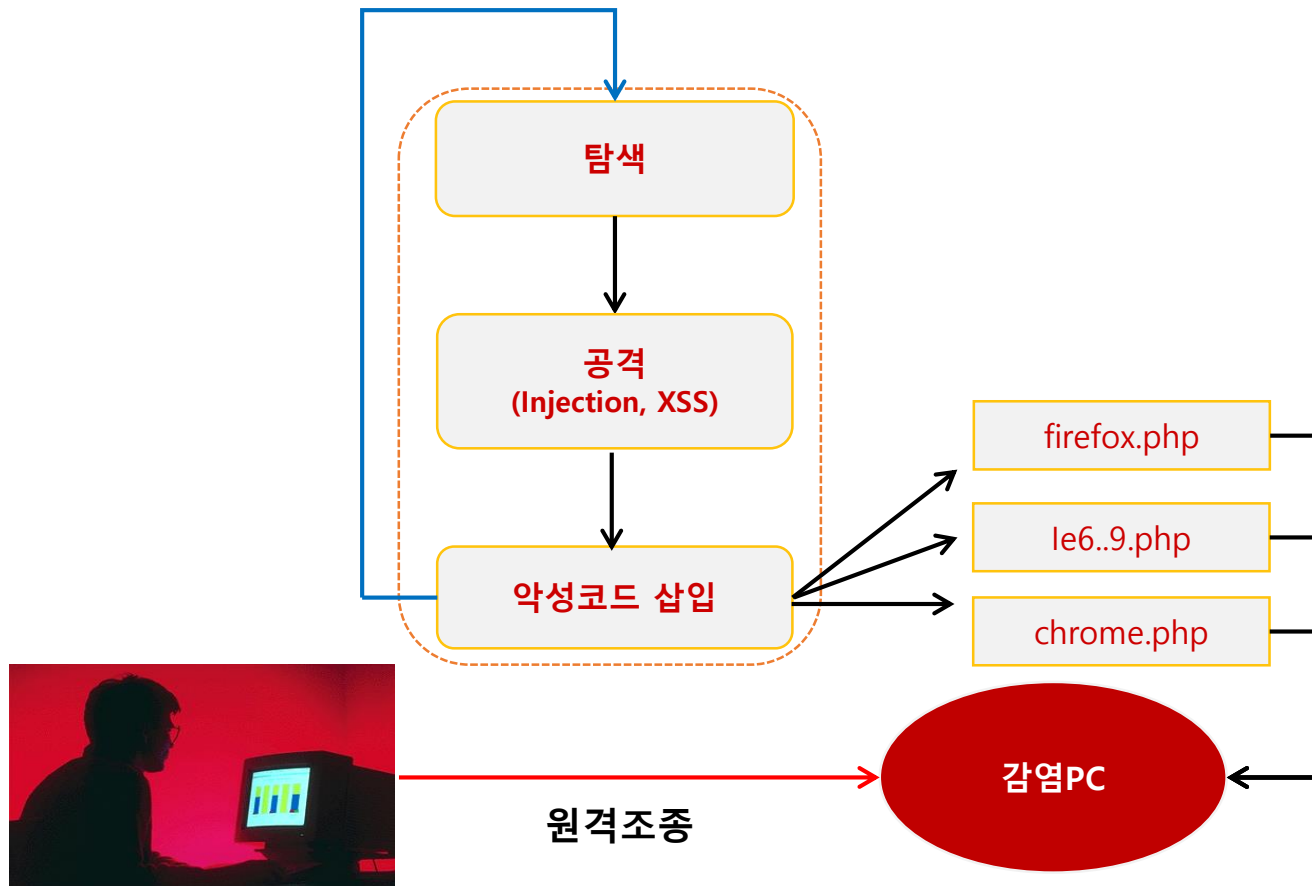
# APT Attack 다양한 프로세스

## APT 공격 프로세스



(자료제공: 시만텍)

# APT Attack 다양한 프로세스



# APT Attack 대상

정부기관

정부기밀문서 탈취  
군사기밀문서 탈취

기업

기업 지적 자산 탈취  
기업 영업 기밀 탈취

금융

금융시스템의 동작 불능  
금융 자산 정보 탈취

산업시설

사이버 테러  
산업시스템의 동작 불능

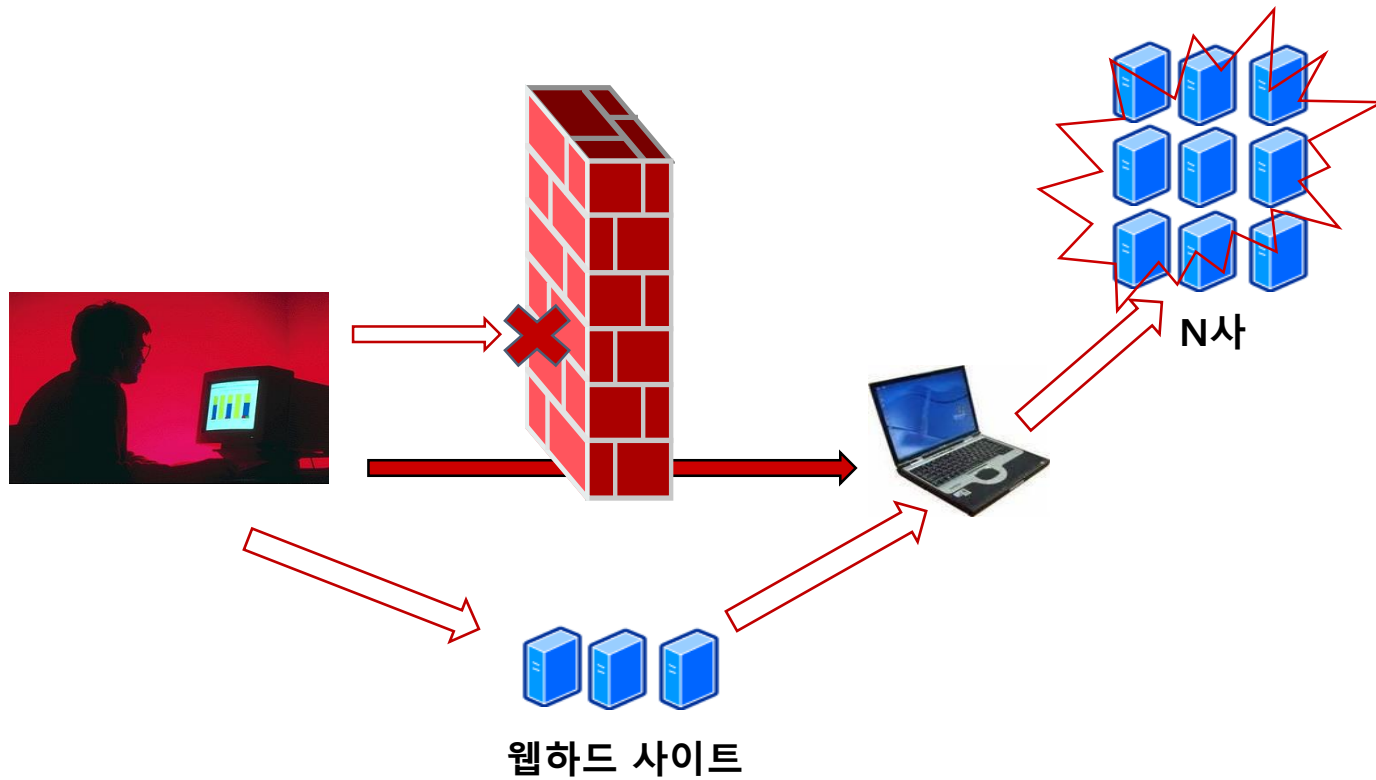
개인

DDOS  
금전적 자산 탈취

# APT Attack 사례 #1

- N 금융사 전산망 해킹 (사이버 테러형 APT 공격)
  - 내역
    - 2011년 4월 12일 17시 10분
    - N사 전산망의 금융서버
  - 공격방법
    - S웹 하드 사이트의 업데이트 프로그램으로 위장된 악성코드 유포
    - 노트북의 주인이 농협시스템 관리자인 걸 알게 된 해커는 7개월간 노트북을 모니터링
  - 피해내역
    - 내부 서버 587대중 273대의 서버의 디스크 손상
    - Web서버 98대중 45대
    - 내부서버 440대중 180대
    - 테스트서버 49대중 48대
    - 재해복구용 서버파괴
    - 2주간의 영업불가, 최소 80억의 피해 발생

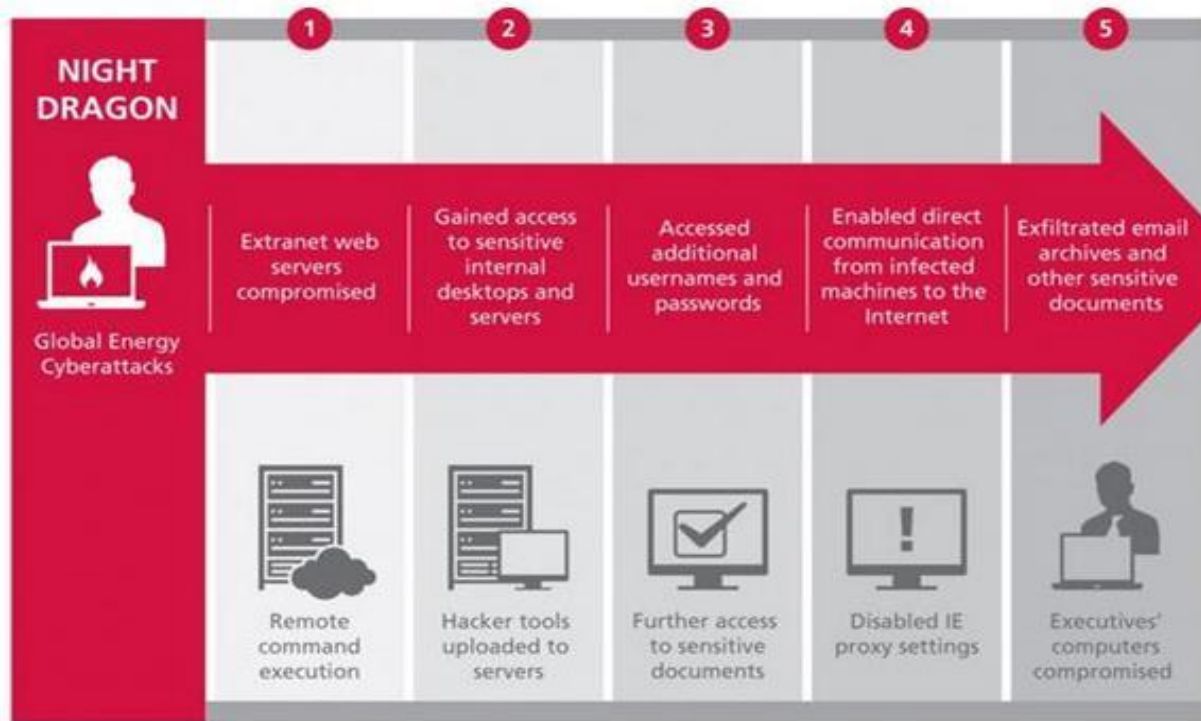
# APT Attack 사례 #1



# APT Attack 사례 #1

- S 웹하드사의 보안관리 실태
  - 77 DDOS 대란때에도 S웹하드사를 통해 악성코드가 유포됨
- N사의 비밀번호 관리 부실
  - 2010.7 이후 변경 사실이 전혀 없음, 관리대장에는 매월 변경한 것으로 허위기재
  - 비밀번호가 유추해내기 쉬운(aaaa,1111) 비밀번호가 대다수
- 직원관리 소홀
  - 외부 유지보수업체 직원들이 무선랜/무선인터넷 이용시에는 승인을 받아야 함에도 노트북 등에서 승인없이 자유롭게 무선인터넷 사용
  - 보안 프로그램이 설치되지 않은채 자유로운 내/외부망 접속
  - 승인없이 자유로운 외부 반출

# APT Attack 사례 #2



Source: McAfee, Inc.  
Anatomy Of The Night Dragon Attack

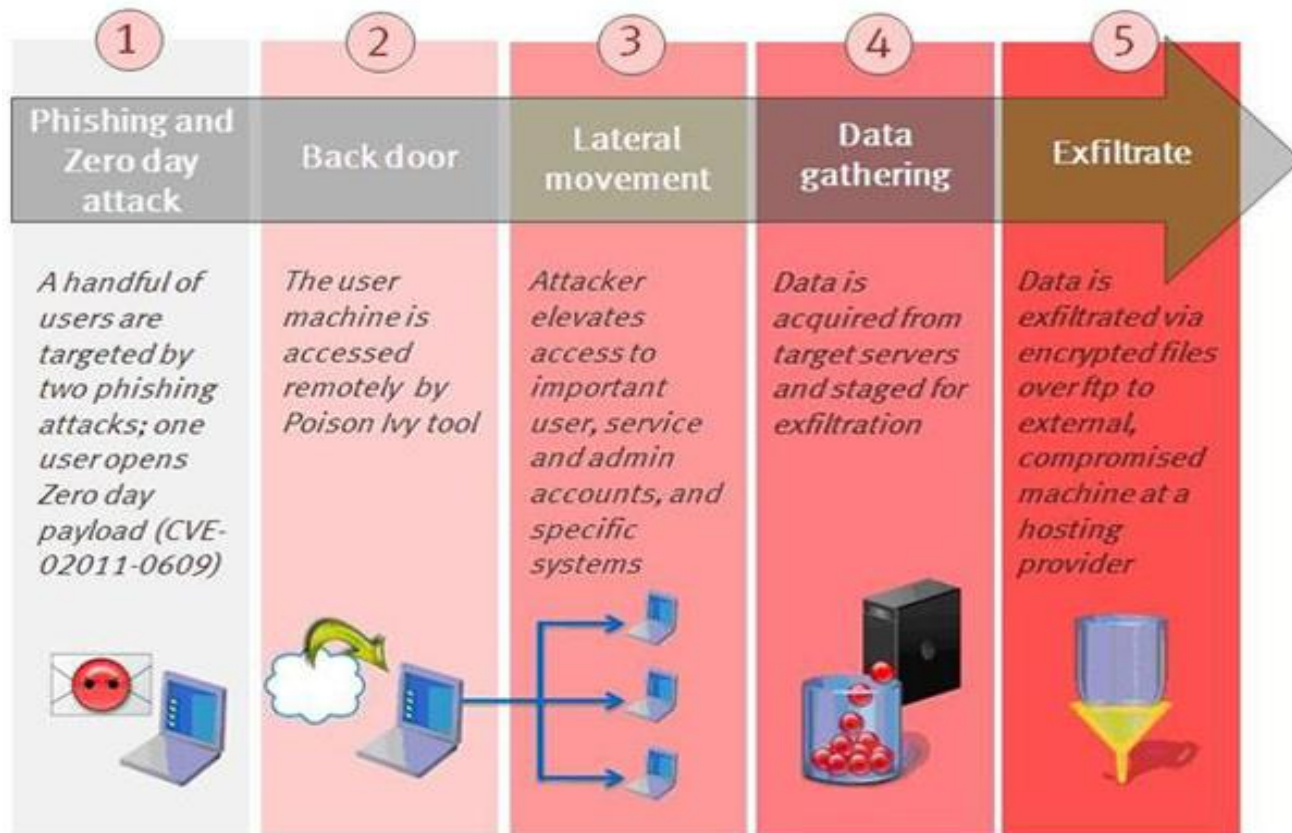
글로벌 에너지 업체 APT공격(나이트 드래곤 공격)

# APT Attack 사례 #2

- 글로벌 에너지 업체 APT공격(나이트 드래곤 공격)
  1. SQL Injection 공격을 통해 악성코드 삽입
  2. 임직원들을 대상으로 타깃 공격을 수행하여 웹서버를 통한 감염
  3. 원 노트북을 이용해 내부 네트워크 접속 시도
  4. 내부 네트워크의 중요시스템 계정 및 비밀번호 획득
  5. 기밀 문서 탈취



# APT Attack 사례 #3



RSA APT공격

# APT Attack 사례 #3

- RSA APT공격

1. 소셜 네트워크 서비스(SNS)를 통한 직원 Email 획득
2. 임직원들을 대상으로 swf(Flash) 0-day 가 첨부된 Email 발송
3. 원격제어 악성코드 감염
4. 내부 네트워크 계정 및 비밀번호 획득
5. 기밀문서 탈취