웹 해킹 스킬업 과정

강사 이세영

Agenda

1. 해킹 및 보안 개론

2. 웹 해킹

2-1. 웹 구조 익히기

2-2. XSS 기법 실습

3. 문제로 익히는 XSS

Key Point

1. 해킹이 뭔지

2. 해킹은 어떤 형태로 수행하는 건지

해킹하면 떠오르는 키워드

해킹이란 무엇일까요?

해킹 hacking

+ 단어장 저장

표준국어대사전 | 고려대한국어대사전 | 우리말샘

명사

1. 정보·통신 다른 사람의 컴퓨터 시스템에 무단으로 침입하여 데이터와 프로그램을 없애거나 망치는 일.

출처 : 표준국어대사전

해킹 hacking

+ 단어장 저장

표준국어대사전 | 고려대한국어대사전 | 우리말샘

명사

수단 목적

1. 정보·통신 다른 사람의 컴퓨터 시스템에 무단으로 침입하여 데이터와 프로그램을 없애거나 망치는 일.

출처 : 표준국어대사전

해킹의 목적

목적	설명
시스템 파괴	✓ 시스템 파괴(운영체제 부팅 실패)
Lateral Movement	✓ 해킹한 단말에서 접근 가능한 다른 자산을 해킹하여, 해당 자산으로 이동하는 공격 기법
모니터링	✓ 회사 망 등 중요 자산에 접근하는 순간까지 기다리는 경우 ✓ 혹은 변태거나..
금전적 목적	✓ 랜섬웨어에 감염시켜 금전적 이득 얻기 ✓ 자료 유출

해킹사고의 관점

목적	설명
공격자 관점	✓ 시스템의 취약한 부분 탐색 및 분석 ✓ 해당 취약점을 악용한 공격 코드(Exploit) 작성
방어자 관점	✓ 공격(침입)이 발생한 시점에서 실시간으로 방어하는 포지션(보통 보안관제)
분석가 관점 (사후 대응)	✓ 사고 발생 이후 시점에서 어떤 피해가 발생했는 지 조사/분석하는 포지션 ✓ 재발 방지를 위한 대책 및 가이드라인을 작성

해킹과 취약점

취약점

설명

✓ 보안상의 문제점을 안고 있는 컴퓨터 시스템의 약점. 컴퓨터 사회가 갖는 취약성에는 외적 요인과 내적 요인의 두 가지로 생각된다. 외적 요인이란 컴퓨터에 대한 범죄 행위나 자연 재해와 같이 컴퓨터 그 자체에 외부로부터 가해지는 것에 대한 취약성이다. 컴퓨터에 관련된 범죄나 컴퓨터의 고장에 의한 사회의 혼란 등이 컴퓨터 사회의 취약성으로 눈을 돌리게 하는 요인이 되고 있다. 한편, 내적 요인이란 컴퓨터 스스로가 만든 취약성이다. 예를 들면 데이터의 집중이나 컴퓨터 센터의 지리적 집중 등이 취약성을 만드는 내적 요인이 될 수가 있다.

[네이버 지식백과] 취약점 [vulnerability] (컴퓨터인터넷IT용어대사전, 2011. 1. 20., 전산용어사전편찬위원회)

해킹과 취약점

	설명
취약점	✓ 개발자가 의도하지 않은 행위를 수행할 수 있는 지점

취약점의 종류

Memory Corruption

메모리를 덮어쓰는 취약점

- ✓ 대상 : Binary
- ✓ 특징 : 고려해야할 점이 많음
- ✓ 주요 영향 : 권한 상승(LPE), 원격 명령 실행(RCE)

다양한 메모리 보호기법 우회(필요)

- ✓ Canary
- ✓(K)ASLR
- ✓ DEP(Data Execution Protection), NX
- ✓ etc

Logical Error

개발자의 실수로 발생하는 취약점

- ✓ 99%의 웹, 앱 취약점이 해당

그럼 공격자 관점에서 생각해봅시다.

가능한 침투 시나리오

APT Attack

Lateral Movement

Supply Chain Attack

가능한 침투 시나리오(Verbose)

APT Attack
→ Browser Exploit, Spear Phishing(Malicious Code), Service Exploit

Lateral Movement
→ SMB, Botnet, etc

Supply Chain Attack

APT Attack

Advanced : **고도화** 된 기법을 통해

Persistent : **지속적**으로

Threat : 대상을 위협하고, **목적을 성취**한다.

APT Attack

Advanced : **최신 공격 기법, 알려지지 않은 취약점**(0-day exploit)

Persistent : **지속적**으로(잠복, 장기간 정보 수집, 사회 공학 기법 등)

Threat : **특정 직원을 대상**으로 기밀 정보 탈취 등의 **목적을 성취**한다.

APT Attack 공격 대상

금융 시스템 마비
금융 자산 정보 탈취

주요 시스템 마비
군/정부 기밀 정보 탈취

지적 재산 탈취
영업 기밀/대외비 탈취

사이버 테러
산업 시스템 마비

금전적 자산 탈취

APT Attack


APT 공격 프로세스
1
침투
공격자가 취약한 시스템이나 직원들을 악성코드로 감염시켜 네트워크 내부로 침투
2
검색
침투한 내부 시스템 및 인프라 구조에 대한 정보를 수집한 후 다음 단계를 계획
3
수집
보호되지 않은 시스템 상의 데이터 수집 또는 시스템 운영 방해
4
유출
공격자의 근거지로 데이터 전송
시스템 운영 방해 또는 장비 파괴
(자료제공: 시만텍)

APT Attack(침투)

침투 전 자료수집(Foot Printing)

대상 → 개인, 기업 모두

방법

1. 명확하게 필요한 정보를 취급하는 타겟을 목표로 설정

2. 해당 사용자의 홈페이지, SNS, 검색 등을 활용해 정보를 획득

APT Attack(침투)

침투 전 자료수집(Foot Printing)

IP를 획득한 경우, 포트 스캐닝 등의 방법을 통해 동작 중인 서비스의 정보를 획득할 수 있음.
→ OS 종류 확인 가능, 서비스 취약점을 사용 가능할 수도 있음

IP를 획득하지 못한 경우, 목표가 악성 행위에 노출되게 만들어야 함.
→ 사회 공학 기법(특히, Spear Phishing), Watering Hole 등의 공격 기법 사용

APT Attack(침투)

사회공학기법

- Spear Phishing

- 악성 파일을 첨부하거나 악성 링크를 첨부하고, 실행하거나 접속하도록 유도

인젝션

0-day Exploit

- 보고되지 않은 서비스 취약점을 활용

- 보고되지 않은 소프트웨어 취약점 사용

APT Attack(검색)

내부 망의 다른 PC로 이동해야하는 경우에 해당

잠복하며, 모니터링(내부 망에 존재하는 **다음 목표 PC에 대한 정보를 수집**) 수행.

해당 단계에서 다른 PC로 이동할 필요가 없다면, 권한 상승을 수행
- 관리자 계정 생성
- Windows System이면 UAC Bypass
- Linux System이면 Service 취약점, Kernel 취약점 사용

APT Attack(수집)

목표가 자료 탈취인 경우, **필요한 자료를 수집**하는 절차

목표가 자료 탈취가 아닌 경우, 어떠한 서비스를 방해하거나 파괴해야 **효율적인지 정보를 수집하고 분석**

검색 단계에서 계정을 획득하지 못했다면, **내부 계정을 획득하고, 권한 상승 수행**
- 내부 계정 획득을 위해 Brute Force Attack 등 사용
- Windows System이면 UAC Bypass
- Linux System이면 Service 취약점, Kernel 취약점 사용
- 관리자 계정 생성

APT Attack(유출)

정보 탈취, 시스템 파괴, 서비스 방해 등 목표를 달성하는 단계

목표를 달성한 뒤 로그 삭제와 같은 “안티 포렌식”을 수행

APT Attack(Case 분석 #1)

목표 : N사 전산망 금융 서버

공격 방법
- 해커는 웹 하드(P2P) 사이트에 업데이트 프로그램으로 위장해서 악성 코드 유포

- 노트북 주인이 N 사의 시스템 관리자인 걸 알게 된 해커는 7개월 간 노트북을 모니터링

피해 내역
- 내부 서버 587대중 273대의 서버의 디스크 손상

- 2주 간 영업 불가, 최소 80억의 피해 발생

APT Attack(Case 분석 #1)

APT Attack(Case 분석 #1)

원인

웹 하드 사이의 보안관리 실태(7·7 DDoS 때도 웹 하드를 통해 유포)

N 사의 비밀번호 관리 부실
- 비밀번호 변경 대장 허위 기재
- 쉬운 패스워드

엄격하지 않은 보안 정책 및 직원들의 보안 의식
- 인트라넷 / 인터넷 망 보안 소프트웨어가 설치되지 않은 상태로 이용
- 허가 없이 무선 인터넷 사용 등

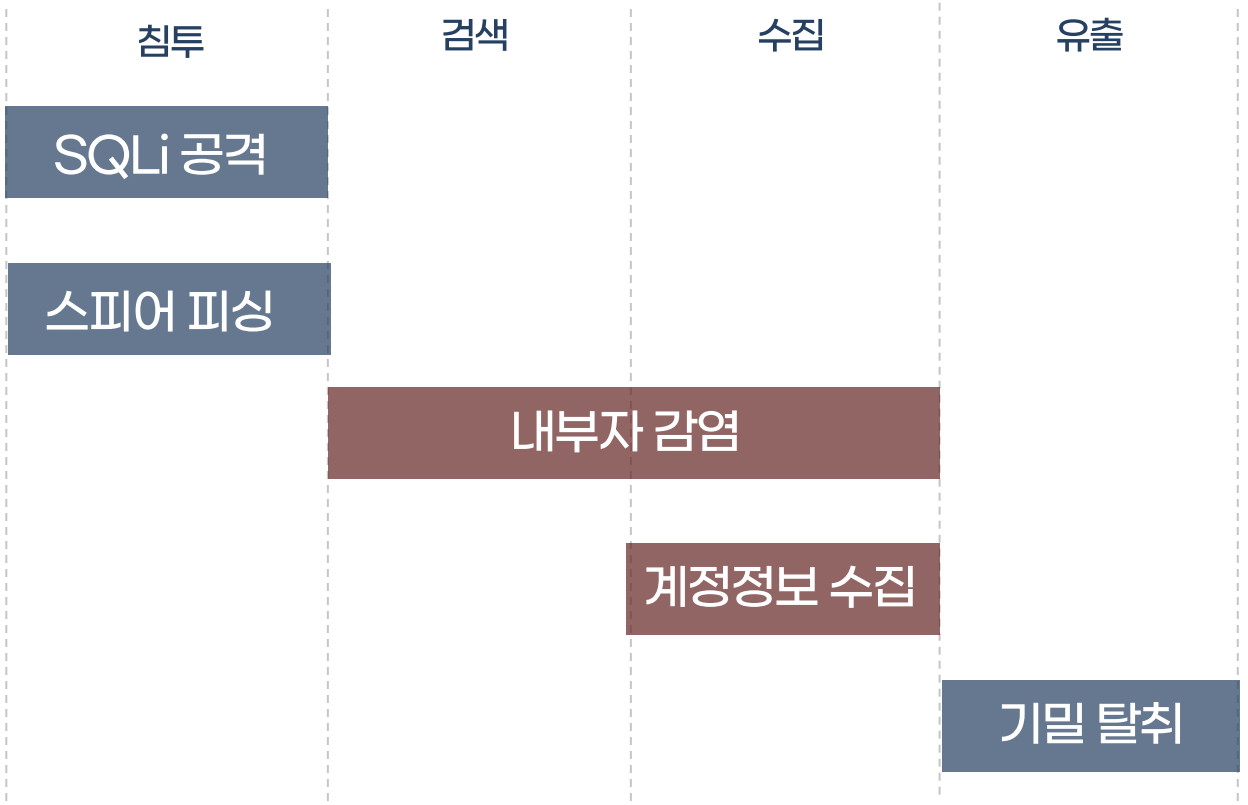
APT Attack(Case 분석 #2)

목표 : 글로벌 에너지 업체(Night Dragon Attack)

공격 방법

- SQL Injection 공격으로 웹 서버에 악성코드 업로드
- Spear-Phishing을 통해 내부자의 계정정보를 획득하고, 악성코드 감염을 시도
- 획득한 계정 정보로 내부 네트워크에 접속, 시스템 내부의 추가적인 사용자 계정 정보 수집
- 시스템을 C2로 연결
- 정보 탈취

APT Attack(Case 분석 #2)



APT Attack(Case 분석 #2)

특징

사회 공학 기법

윈도우 취약점

Active Directory 환경

RAT(Remote Administaration Tool)

APT Attack(가상 Case)

Keywords

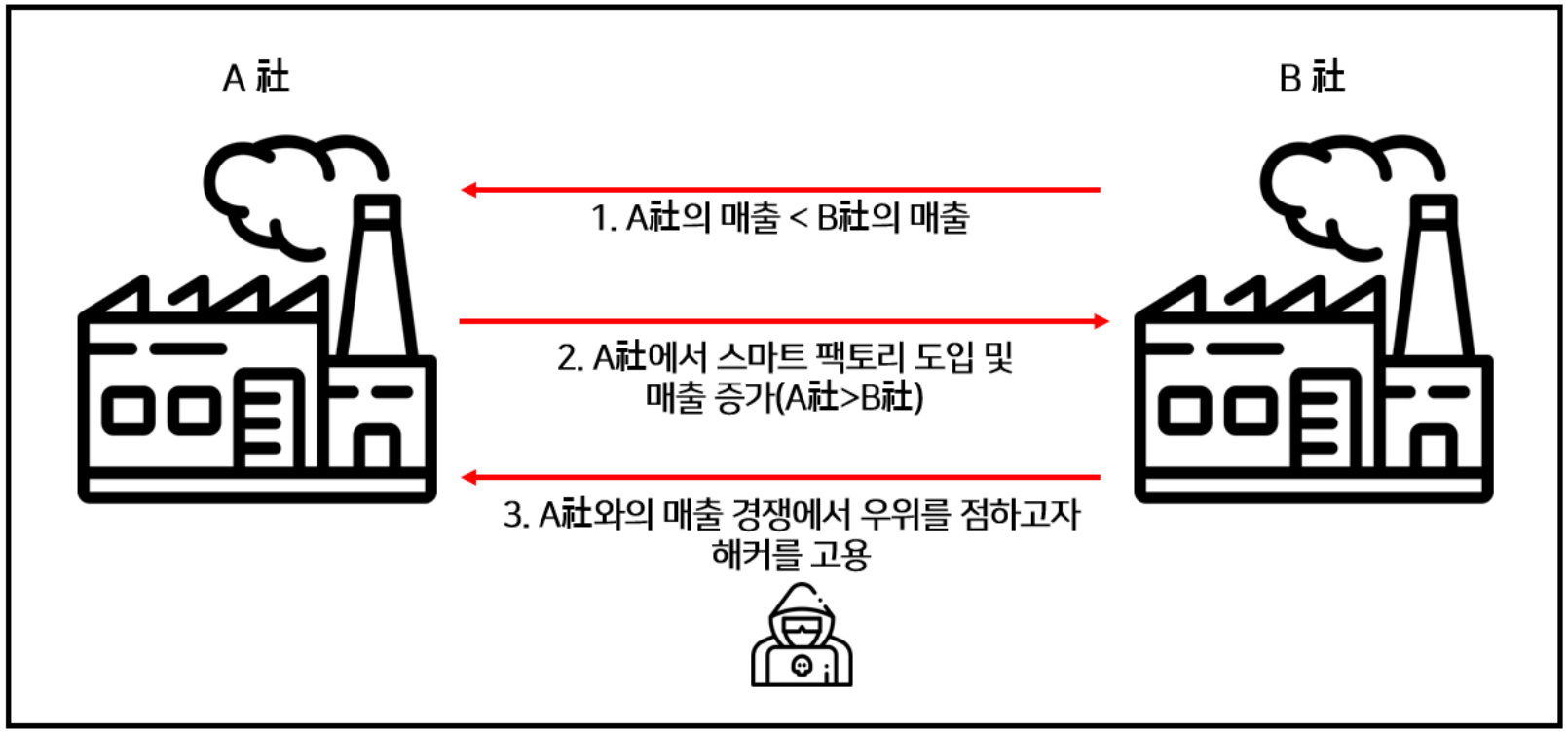
Spear Phishing

Lateral Movement

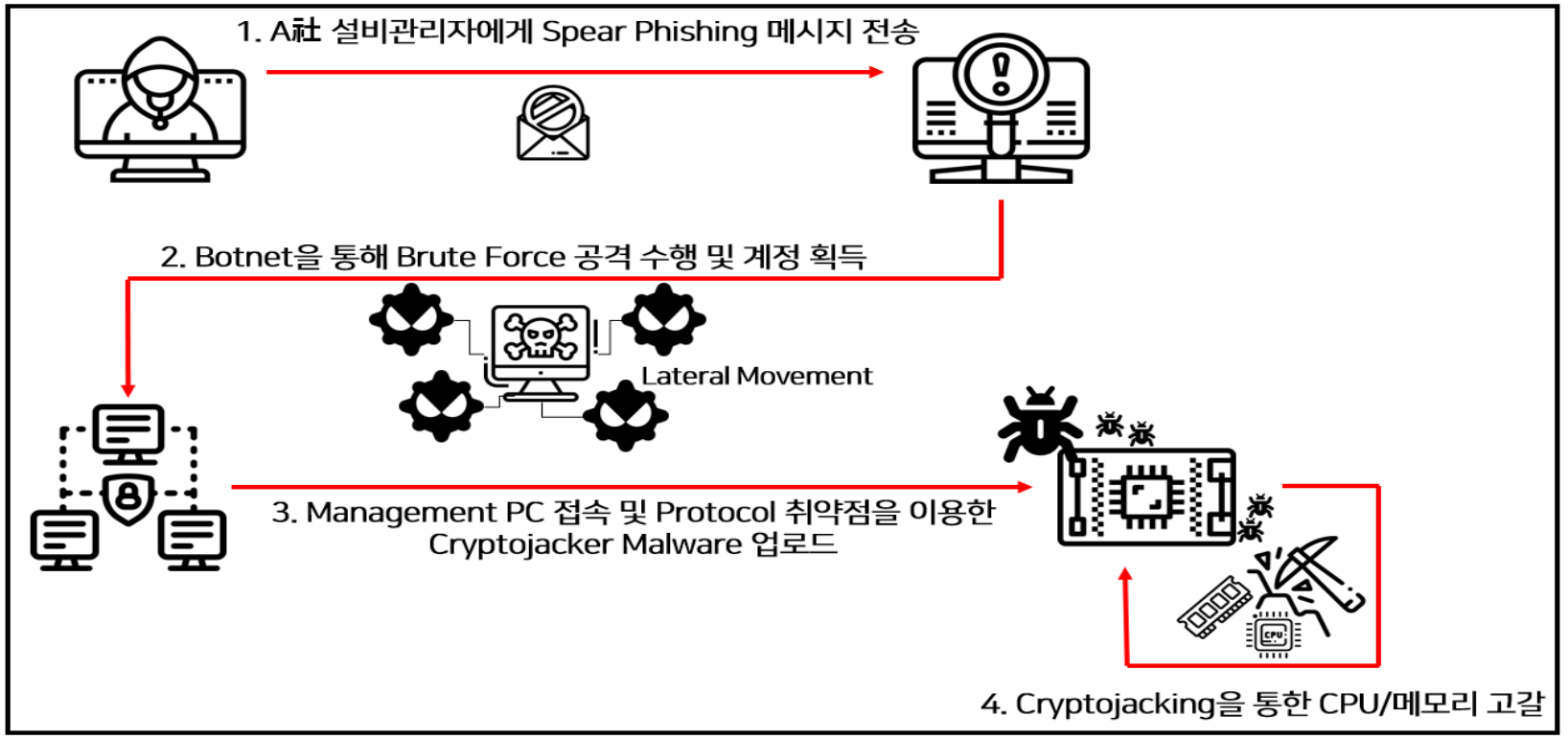
Supply Chain Attack

Crypto Jacking

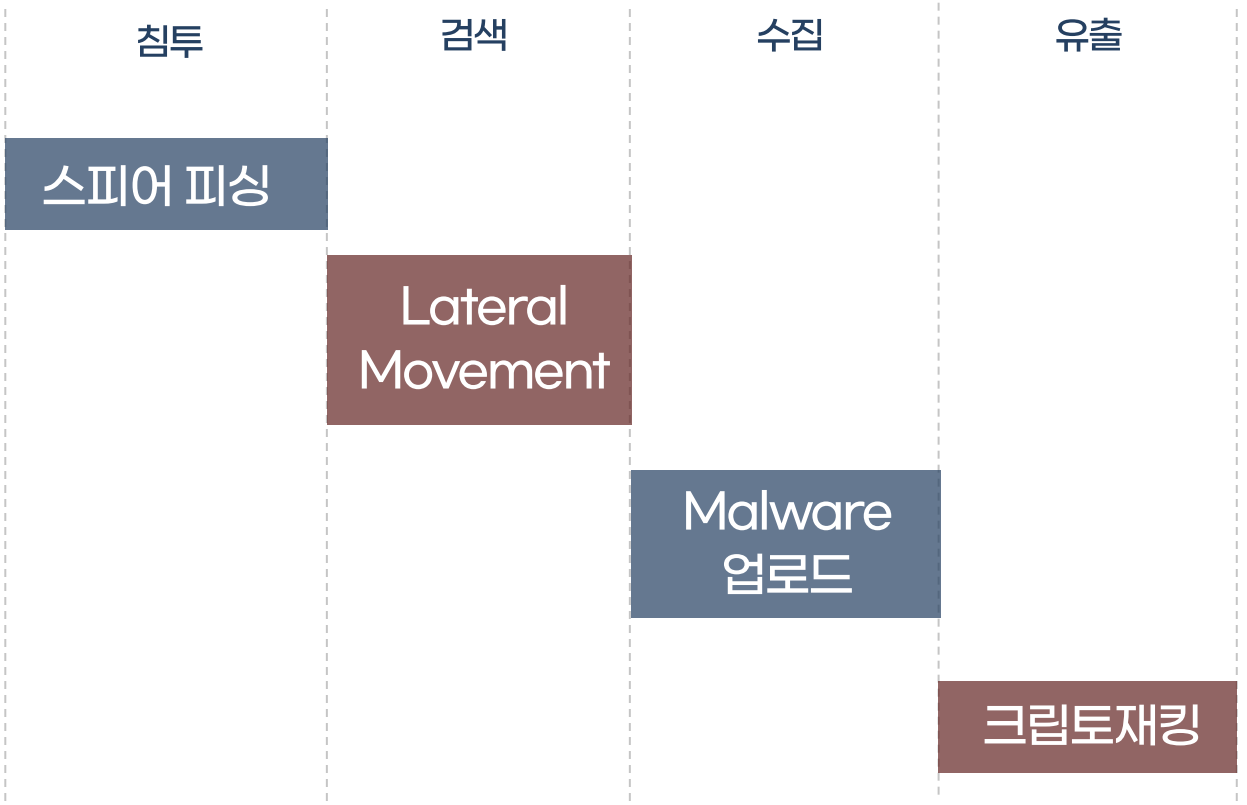
APT Attack(가상 Case)



APT Attack(가상 Case)

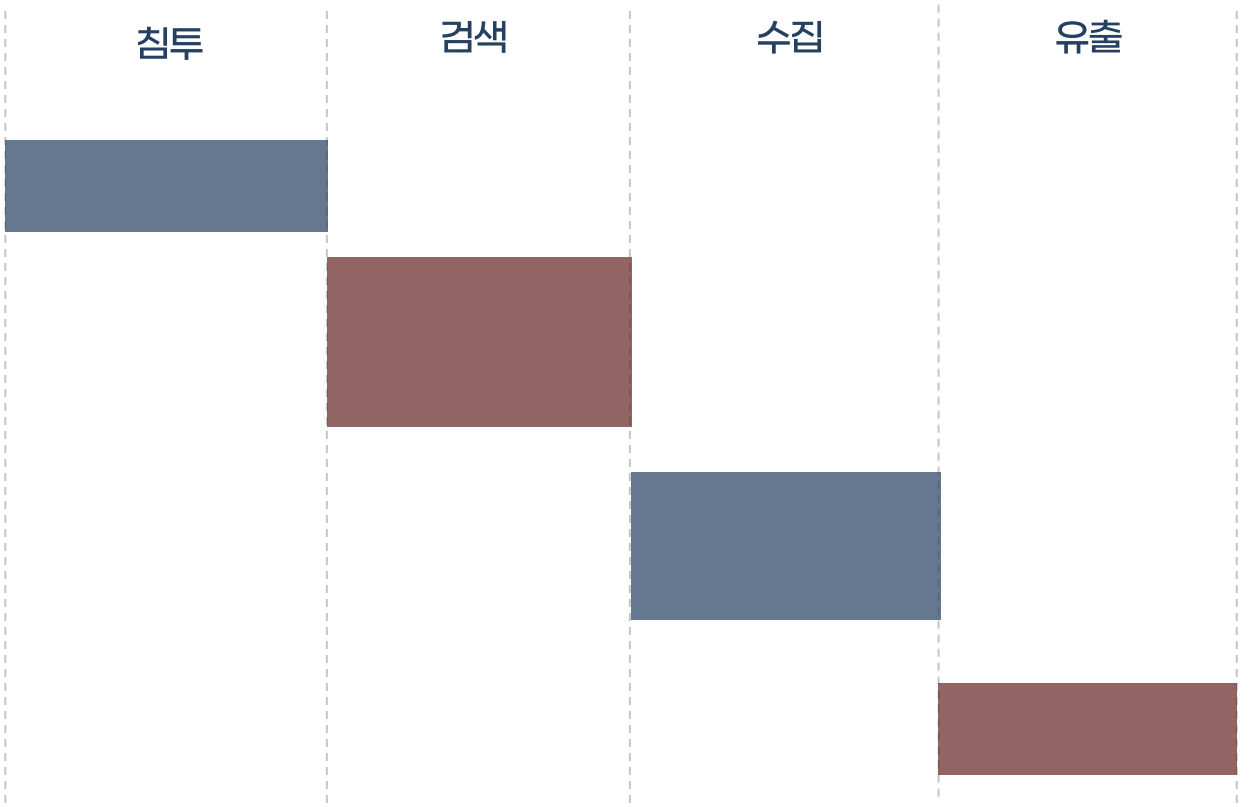


APT Attack(가상 Case 분석)

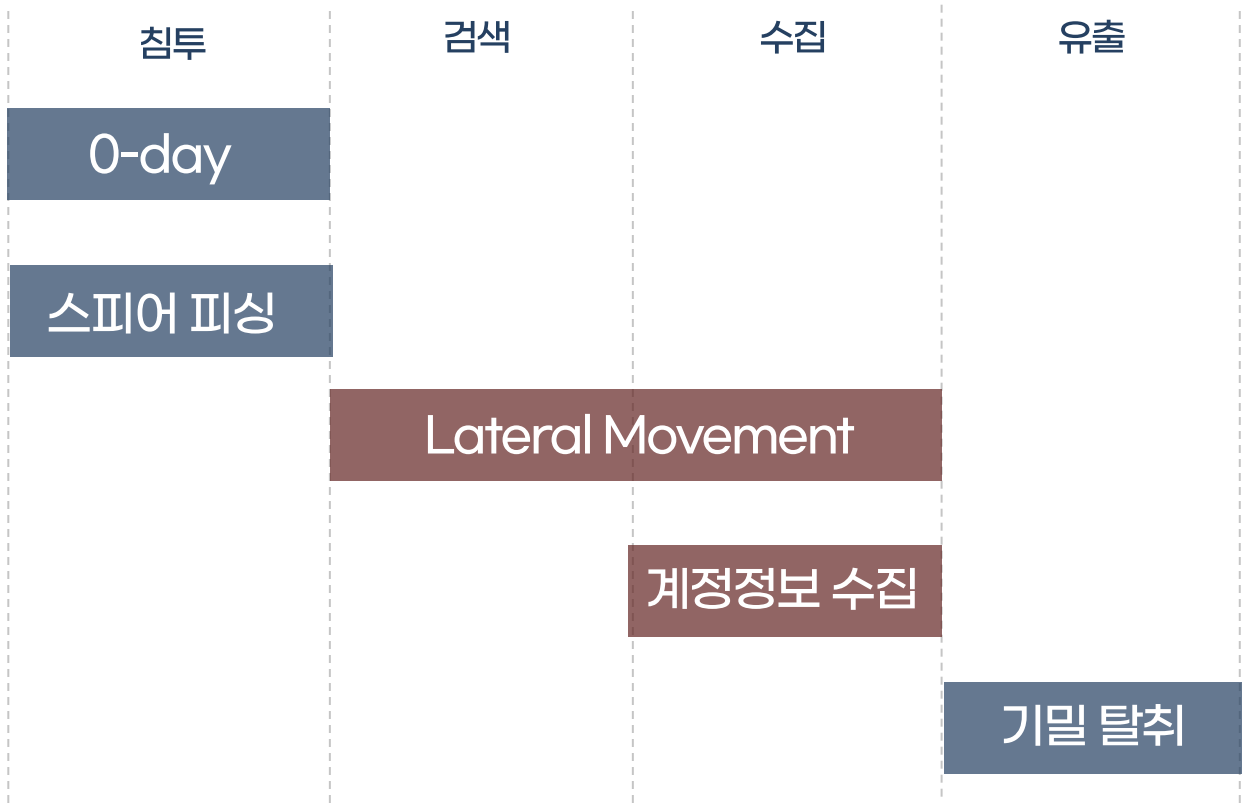


공격자 관점에서의 공격 과정

시나리오 설계



APT Attack



APT Attack

침투 전 자료수집(Foot Printing)

IP를 획득한 경우, Service Exploit(특히 RCE)을 해볼 수 있음

IP를 획득하지 못한 경우, 목표가 악성 행위에 노출되게 만들어야 함.
→ 사회 공학 기법(특히, Spear Phishing), Watering Hole 등의 공격 기법 사용

공격자 관점에서의 공격 과정

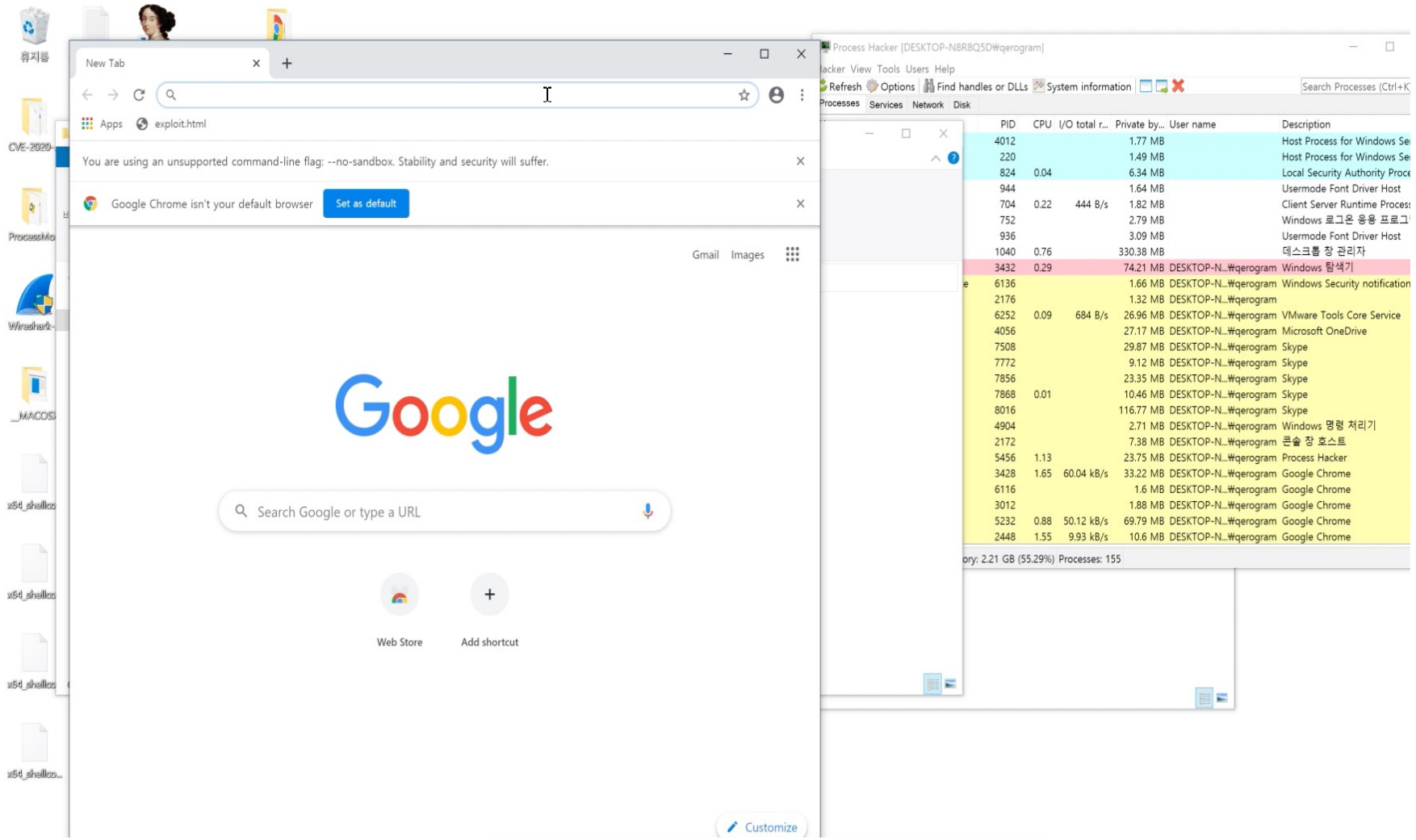
시나리오 설계(침투)

1. Browser Exploit
   [조건] 사용자가 사용할만한 브라우저를 맞춰야 함.
   [조건] 상대가 해당 링크에 접속을 해야 함

2. Spear Phishing
   [조건] 악성코드 만들기
   [조건] 상대가 읽고 실행하게 만들어야 함

공격자 관점에서의 공격 과정

시나리오 설계(침투) - Browser Exploit (Chrome)



그럼 분석가 관점에서 생각해봅시다.

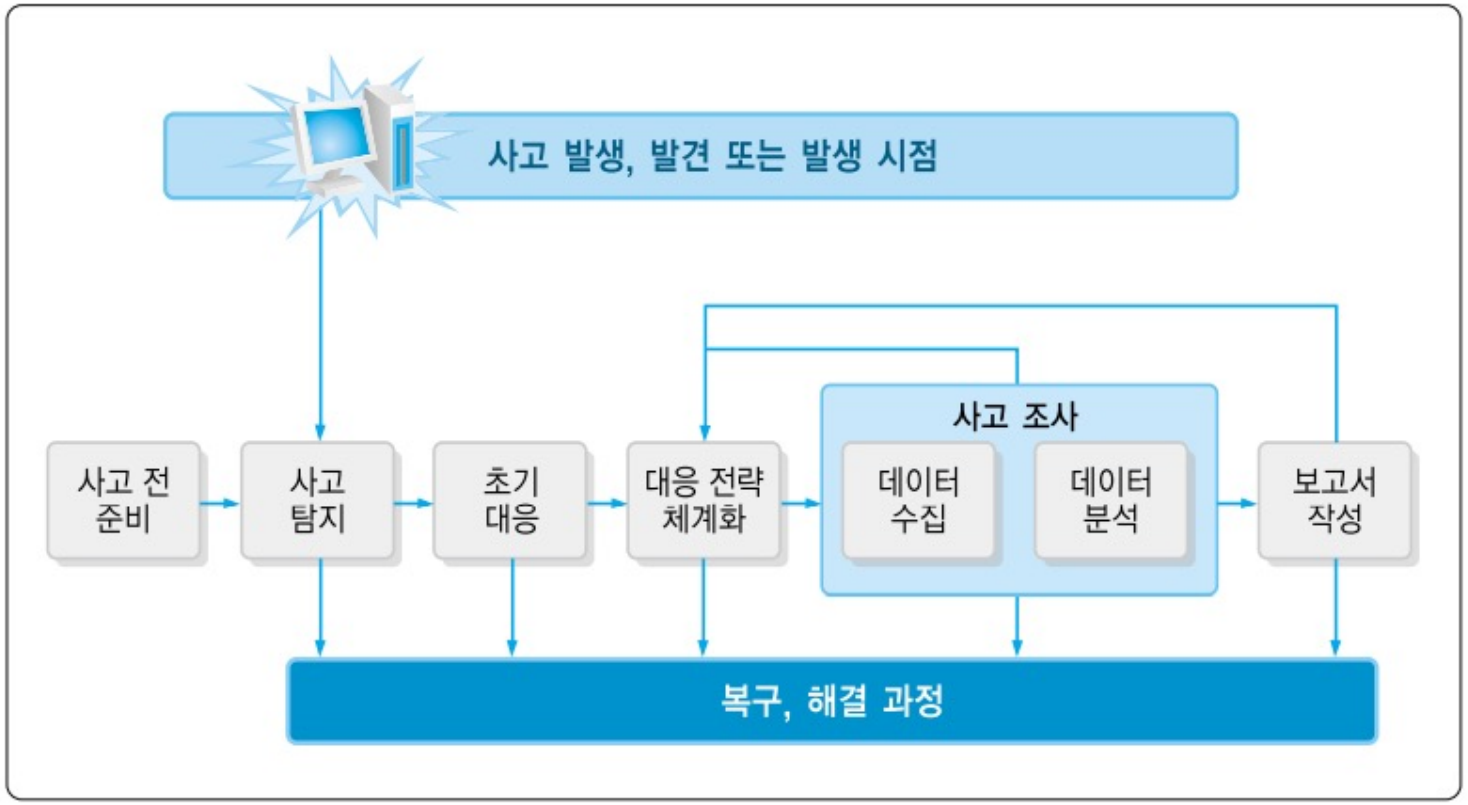
침해사고

해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등에 의하여
정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인해 발생한 사태

정보통신망법 제2조 1항 7조

특징별 침해사고
대규모(다수의 서버를 동시에 공격)
분산화(다수의 서버에서 목표시스템을 공격)
대중화(해킹 관련 정보의 손쉬운 획득)
범죄적 성향(금전적 이익, 산업정보 침탈, 정치적 목적)

- KISA 침해사고 분석 절차



- KISA 침해사고 분석 절차

용어 정리

	설명
어택 벡터	✓ 취약점이 존재하는 지점
Payload	✓ 공격자가 네트워크를 통해 전송할 악의적인 코드 ✓ 공격 후 하는 모든 행위 자체를 Payload라고 하기도 함.
Exploit	✓ 취약점을 트리거 할 수 있는 코드 악용(사용)하는 행위 활용) 익스를 뜬다, 익스를 짠다, 익스했다. 등

Key Point

1. 웹이 어떻게 구성되어 있는지

2. 웹 해킹이 어떤 것인지

웹하면 떠오르는 키워드

웹이란 무엇일까요?

웹

설명

우리가 흔히 사용하는 “인터넷에서 확인해 볼게요”라는 말의 뜻은 “인터넷 익스플로러나 크롬 등의 웹 브라우저를 통해 웹 사이트에 접속하여 내용을 확인해 볼게요”의 뜻입니다.
즉, 인터넷과 웹을 비슷한 의미로 섞어서 사용하고 있는 것이지요.

하지만, 실은 **인터넷과 웹은 동일한 의미가 아니랍니다.**
인터넷은 컴퓨터 네트워크 망 자체를 의미하며, **웹은 인터넷 상에서 동작하는 하나의 서비스**일 뿐입니다. 인터넷을 이용하여 할 수 있는 서비스로는 전자우편(e-mail), 파일전송(FTP), 원격접속(telnet), 유즈넷(usenet) 등 다양한 서비스가 있답니다. 그중 현재 가장 많이 사용되는 서비스가 웹(web)이라 할 수 있지요.

[네이버 지식백과] 웹 [World Wide Web] (소프트웨어 어휘다지기 - 중등)

웹과 서비스

	설명
웹	✓ 파일 ✓ 웹 브라우저를 통해 렌더링 되어 보여질 프로그램 코드
서비스	✓ 외/내부에서 접근할 수 있는 프로세스
프로그램	✓ 실행되지 않은 상태의 파일 ✓ 비휘발성 메모리(SSD, HDD)에 적재되는 형식
프로세스	✓ 실행된 상태의 프로그램 ✓ 메모리(휘발성)에 프로그램이 적재되는 형식

웹과 서비스

	설명
서버	✓ 서비스가 실행된 주체(컴퓨터, 폰 등)
클라이언트	✓ 서비스를 이용하는 고객 ✓ 웹 서비스를 이용할 때는 일반적으로 웹 브라우저를 사용
아이피	✓ 컴퓨터를 찾을 수 있는 주소(공인 / 사설)
포트	✓ 컴퓨터로 접근할 수 있는 문(1 - 65535)

웹을 만들기 위한 3요소

HTML

설명

- ✓ 파일
- ✓ 웹의 기틀을 잡음
- ✓ Tag로 구성됨.
- ✓ Tag는 0개 이상의 Attribute를 가질 수 있음.

형태

```
<html>
    <head></head>
    <body>
        <img src='hello.jpg'/>
    </body>
</html>
```

웹을 만들기 위한 3요소

CSS

설명

- ✓ 파일
- ✓ HTML 요소를 꾸미는 용도
- ✓ Style Tag 혹은 Style Attribute로도 사용될 수 있음

형태

```
img {
    width: 1024px;
}
```

웹을 만들기 위한 3요소

JavaScript

설명

- ✓ 파일
- ✓ 웹에서 대부분의 기능을 담당
- ✓ 스크립트 기반의 언어
- ✓ Script Tag를 통해 사용할 수 있음.

형태

```
let t = '안녕하세요';
alert(t);
```

로그인 페이지를 만들며 HTML/CSS/JS 이해하기 (실습)

XSS

Cross Site Script

악의적 js를 실행시키자

- ✓ 대상 : Web Server
- ✓ 목적 : 계정 탈취

XSS

XSS

설명

Cross Site Script의 약자

주요 목적 : 계정 탈취

개발자가 의도하지 않은 악의적인 Javascript를 삽입하고 실행하는 공격 기법

시나리오 1) 특정 페이지에 접근했을 때, 내 게시글이 삭제되는 경우

시나리오 2) 특정 페이지에 접근했을 때, 다른 페이지로 리다이렉션 되는 경우

실습을 통해 XSS를 이해해봅시다.

문제로 익히는 XSS

문제를 통해 XSS를 익혀봅시다.

감사합니다.