|  |
| --- |
| **제목** |

**2019.01.23**

**팀명 :**

**(팀원)**

**개 정 이 력**

|  |  |  |  |
| --- | --- | --- | --- |
| **개정 번호** | **개정 내용 요약** | **추가/수정 항목** | **개정 일자** |
| 0.1 | 최초 작성 |  |  |
| 0.2 | 내용 추가 |  |  |
| 0.3 | 내용 추가 |  |  |
| 0.4 | 내용 추가 |  |  |
| 0.5 | 내용 추가 |  |  |
| 0.6 | 내용 추가 |  |  |
| 0.7 | 내용 추가 |  |  |
| 0.8 | 내용 수정 |  |  |
| 0.9 | 내용 수정 |  |  |
| 1.0 | 내용 수정 |  |  |

**문 서 규 칙**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 제목 | | | 팀명 |
| Category | 첨부파일 버전 | 문서 최종 수정일 |
| ① | ② | ③ |

* 작성 및 확인은 Microsoft Word 2010으로 작성되어 졌으며, Acrobat Reader로 읽는다.
* Category(①)에는 Manual, Utility, Tip, Analysis Report 로 구분하며, 기재된 정보가

Manual과 Utility가 혼합된 경우에는 "Manual + Utility" 라고 표기되며, 머리글의

Category에 해당 구분 정보를 표기된다.

* 첨부 파일 버전(②)은 첨부 파일이 존재하는 경우에 기재되며, 첨부 파일의 버전이

표기된다. (유틸리티의 경우 최종 버전은 날짜 표기 대신 버전으로 대체한다)

* 문서 최종 수정일(③)에는 문서의 최종 수정날짜가 표기된다.

**목 차**

[**1.** **프로젝트 개요** 1](#_Toc534384309)

[**1.1** **주제 선정 및 동기** 1](#_Toc534384310)

[**1.2** **프로젝트 목표** 1](#_Toc534384311)

[**1.3** **AS-IS, TO-BE** 1](#_Toc534384312)

[**1.4** **프로젝트 역할 분담** 2](#_Toc534384313)

[**1.5** **프로젝트 일정** 2](#_Toc534384314)

[**2.** **공격 시나리오** 3](#_Toc534384315)

[**2.1** **개요** 3](#_Toc534384316)

[**2.2** **환경구성** 3](#_Toc534384317)

[**2.2.1** **웹서버** 3](#_Toc534384318)

[**2.2.2** **공격자** 4](#_Toc534384324)

[**2.3** **사용된 취약점 설명** 4](#_Toc534384325)

[**2.3.1** **Adobe Flash Player 취약점(CVE-2015-5122)** 4](#_Toc534384326)

[**2.4** **공격 프로세스** 5](#_Toc534384327)

[**2.5** **시나리오 검증** 5](#_Toc534384328)

[**3.** **개발 내용** 6](#_Toc534384329)

[**3.1** **논리폭탄** 6](#_Toc534384333)

[**3.1.1** **개요** 6](#_Toc534384338)

[**4.** **개발 결과 및 시연** 6](#_Toc534384339)

[**4.1** **결과** 6](#_Toc534384340)

[**4.2** **전체 시나리오 시연** 6](#_Toc534384341)

[**5.** **문제점 및 추후 과제** 6](#_Toc534384342)

[**6.** **참고자료** 6](#_Toc534384343)

[**7.** **붙임** 6](#_Toc534384344)

**표 목 차**

[[표 1‑1] AS-IS / TO-BE 1](#_Toc534384302)

[[표 1‑2] 프로젝트 역할 분담 2](#_Toc534384303)

[[표 2‑1] 웹서버 HW 환경 구성표 3](#_Toc534384304)

[[표 2‑2] 웹서버 SW 환경구성표 4](#_Toc534384305)

[[표 2‑3] 공격자 HW 환경 구성표 4](#_Toc534384306)

[[표 2‑4] 공격자 SW 환경 구성표 4](#_Toc534384307)

**그 림 목 차**

[[그림 1‑1] 프로젝트 일정 2](#_Toc534384476)

[[그림 2‑1] 공격 프로세스 5](#_Toc534384477)

# **프로젝트 개요**

## **주제 선정 및 동기**

* 본 프로젝트는 Kitri Academy에서 진행하는 정보보안 전문가 교육과정에서 진행한 프로젝트 결과에 대한 보고서이다. 본 보고서는 전 교육과정에 대한 실무 응용 능력과 국내 보안 기술 향상에 기여하고자 한다.

## **프로젝트 목표**

* 피해규모 대비 적은 연구 결과

논리폭탄 공격은 피해규모가 큼에도 불구하고 현재 논리폭탄 공격에 대한 국내 연구는 전무한 상황이다. 따라서, 미리 대비하여 큰 피해를 예방하고자 한다.

* 프로그래밍 능력 수준 향상

현재 본 팀의 구성원들은 독립적으로 운영 가능한 보안 솔루션 개발에 대한 경험이 전무하다. 이에 따라 독립적으로 운영 가능한 솔루션을 개발해 봄으로서, 실무 투입시 적응 기간을 줄이고, 개발 능력을 향상시킬 수 있는 기회로 삼는다.

## **AS-IS, TO-BE**

|  |  |
| --- | --- |
| AS – IS | TO – BE |
| * + 상대적으로 부족한 연구, 대비 * 현재 논리폭탄에 대한 탐지   + 팀 개발 능력 저조 * 팀원 전체가 독립적으로 작동 가능한 솔루션에 대한 개발 경험이 전무 | * + 논리폭탄 공격 탐지, 방어 솔루션 개발 * 피해 발생에 대비한 로깅 기능 구현   + 서비스 관리자들의 교육, 인수 인계를 위한 기술 문서 작성 * 전사적 대응을 통한 피해 최소화   + 팀내 개발능력 향상 |

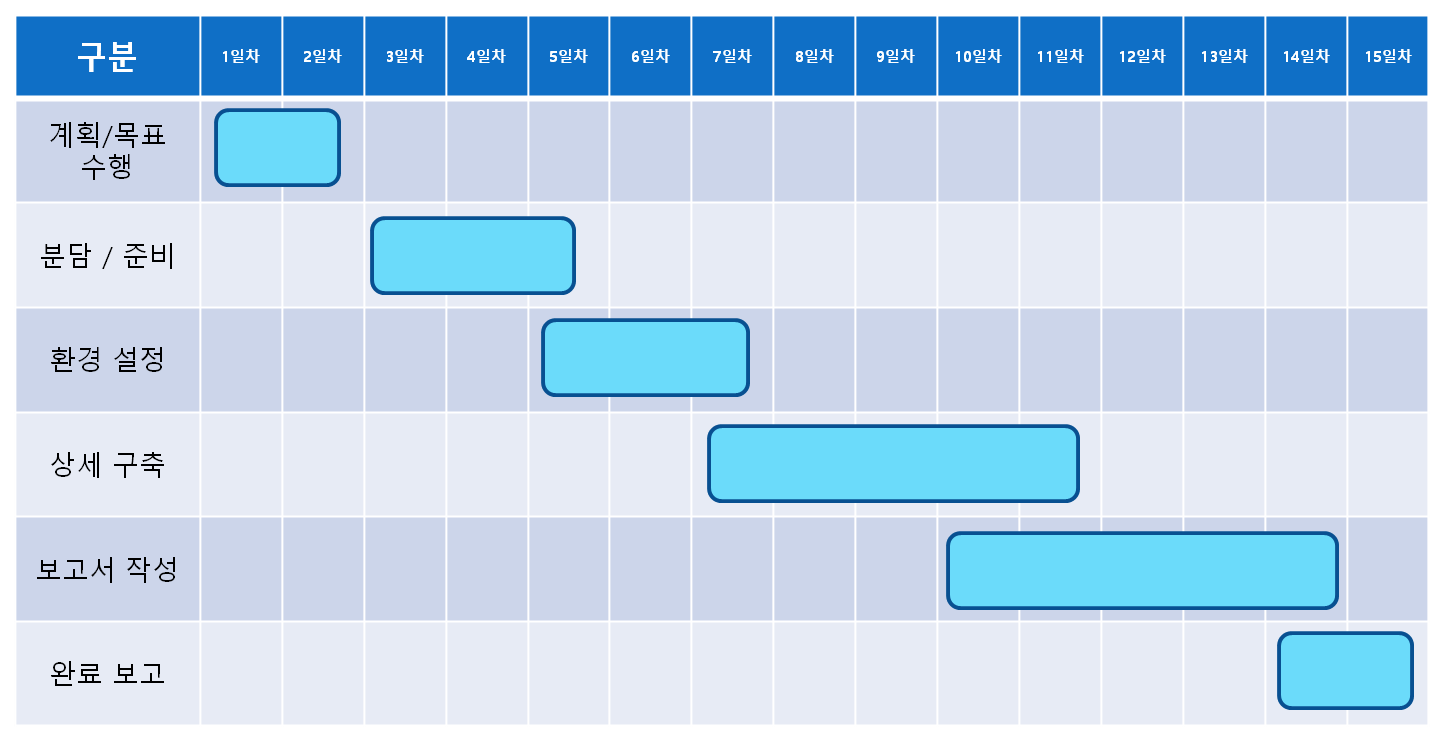
[표 1‑1] AS-IS / TO-BE

## **프로젝트 역할 분담**

|  |  |  |
| --- | --- | --- |
| 이름 | 직책 | 역할 |
|  | PM | 악성코드, 솔루션 개발, 문서작성 |
|  | 팀원 | 악성 스크립트 작성, 웹서비스 구축 및 관리 |
|  | 팀원 | 취약점 코드 분석, 시나리오 작성, 검증 |
|  | 팀원 | 악성코드, 솔루션 개발, 문서작성 |

[표 1‑2] 프로젝트 역할 분담

## **프로젝트 일정**



[그림 1‑1] 프로젝트 일정

# **공격 시나리오**

## **개요**

* qwe

## **환경구성**

### **웹서버**

* HW

|  |  |  |
| --- | --- | --- |
| 이름 | 직책 | 역할 |
|  | PM | 악성코드, 솔루션 개발, 문서작성 |
|  | 팀원 | 악성 스크립트 작성, 웹서비스 구축 및 관리 |
|  | 팀원 | 취약점 코드 분석, 시나리오 작성, 검증 |
|  | 팀원 | 악성코드, 솔루션 개발, 문서작성 |

레이아웃-자동맞춤-고정열너비

|  |  |  |
| --- | --- | --- |
| NAME | TYPE | SPEC |
| DESKTOP PC | CPU | Intel®Core™ i5-2400@3.10GHz |
| RAM | 4GB |
| HDD | 500GB |
| WEB + DB SERVER | CPU | Intel®Core™ i5-2400@3.10GHz |
| RAM | 1GB |
| HDD | 20GB |

[표 2‑1] 웹서버 HW 환경 구성표

* SW

|  |  |  |
| --- | --- | --- |
| NAME | TYPE | SPEC |
| WINDOWS | OS | Version 10 – 64bit |
| Cent OS | OS | Version 6.7 – 64bit |
| KALI | OS | Version 1.0.7 – 32bit |
| APACHE | Application | Version 2.2.15 |
| PHP | Application | Version 5.3 |
| phpMyAdmin | Application | Version 4.0.10.11 |
| MYSQL | Application | Version 14.14 Distrib 5.1.73 |

[표 2‑2] 웹서버 SW 환경구성표

* 공격 대상 웹 서비스는 ‘CoreMall’ 이라는 쇼핑 사이트로, 위에 표기한 환경으로 구성되어 있다.



### **공격자**

* HW

|  |  |  |
| --- | --- | --- |
| NAME | TYPE | SPEC |
| DESKTOP PC | CPU | Intel®Core™ i5-2400@3.10GHz |
| RAM | 4GB |
| HDD | 500GB |

[표 2‑3] 공격자 HW 환경 구성표

* SW

|  |  |  |
| --- | --- | --- |
| NAME | TYPE | SPEC |
| WINDOWS | OS | Version 10 – 64bit |
| KALI | OS | Version 1.0.7 – 32bit |

[표 2‑4] 공격자 SW 환경 구성표

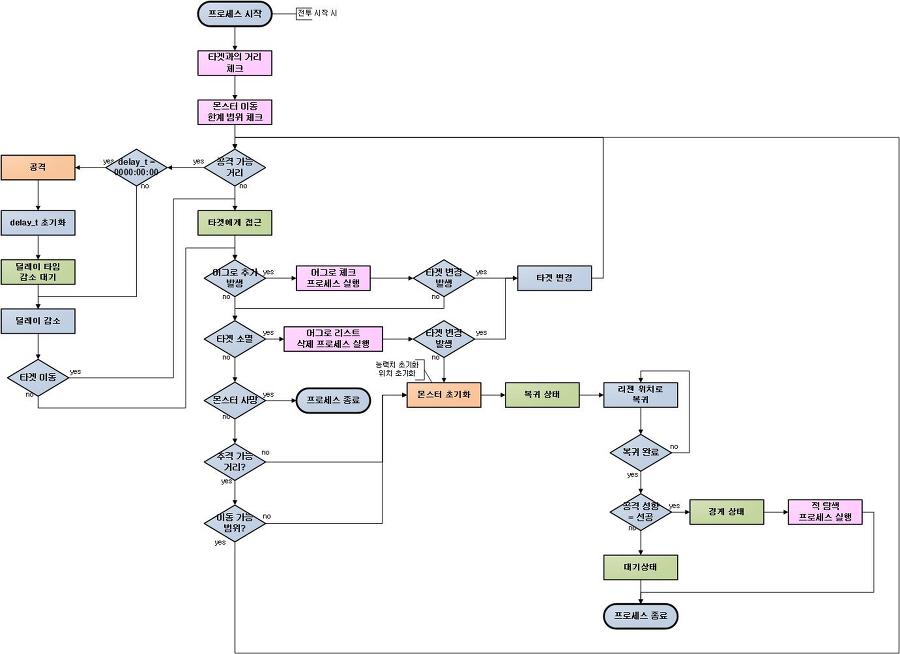
* 공격자는 다른 네트워크상에서 공격 한다고 가정하고, 공격자의 환경 구성은 위와 같다.

## **사용된 취약점 설명**

### **Adobe Flash Player 취약점(CVE-2015-5122)**

* Display

## **공격 프로세스**



[그림 2‑1] 공격 프로세스

## **시나리오 검증**

* 공격자는 metasploit 을 이용하여

# **개발 내용**



## **논리폭탄**



### **개요**

* 예시

# **개발 결과 및 시연**

## **결과**

## **전체 시나리오 시연**

# **문제점 및 추후 과제**

# **참고자료**

# **붙임**