Team No.

TONGMYONG UNIVERSITY

전공연구형_Capstone Design 신청서

과제명	국문	Apache Access.log와 Yara Library를 활용한 웹쉘 탐지에 대한 연구					
	영문	A study on web shell detection using Apache Access log and Yara Library					
과제팀명		술래					
참여학과		정보보호학과	교과목명	DID 인증 기술 _Capstone Design			
지도교수		성명			소속(학과)		
		신 승 수			정보보호학과		
참여 학생	구분	소속학과(전공)	학번	학년	성명	연락처	이메일
	팀장	정보보호학과	18학번	3	강 * *	010-5056-****	kooo1225@naver.com
	팀원	정보보호학과	20학번	3	김 * *	010-4056-****	kimminsu4940@naver.com
		정보보호학과	20학번	3	권 * *	010-4686-****	sang0712on@naver.com
		정보보호학과	19학번	3	권 * *	010-3113-****	ksb010105@naver.com
수행기간		2022년 9월 ~ 2022년 12월					
유형선택		☐ 기업성장형 ☐ 사회기여형 ☐ 창업연계형					
구분 / 지원금액		■ 전공연구형	☐ 과제창출형_C유형 (예산 300,000원)				
			■ 학술연구형_D유형 (예산 200,000원)				

동명대학교 현장실습지원센터 규정에 의거, 캡스톤디자인 과제를 성실하게 수행하고자 본 과제 신청서를 제출합니다.

붙임 : 과제 제안서 1부

2022. 9. 14.

신청인(대표학생) : 강 * * (인)

과제지도교수 : 신 승 수 (인)

동명대학교 현장실습지원센터장 귀하

<별지 제4호 서식> (개정 2018.03.12.) (2019.09.20.) **전공연구형**

Capstone Design 과제 제안서

1. 과제 선정 배경 및 과제 수행 목적

- 2022년 7월경 기업을 대상으로 외부에 노출된 취약한 서버를 경로로 침투한 공격자가 내부 네트워크까지 장악하는 귀신 랜섬웨어 침해사고가 빈번히 발생함.
- 더욱 강력한 침해사고를 일으키기 위해 대부분 해커는 악의적인 목적으로 웹 서버에 악성 코드나 공격 도구를 내려받고 임의의 명령을 실행할 수 있도록 제작한 프로그램인 웹쉘을 이용함.
- 웹쉘이란 공격자가 웹 서버의 업로드 취약점을 통해 시스템에 명령을 내릴 목적으로 만들어진 악성코드이며 일반적으로 웹쉘은 웹 서비스 포트를 통해 이루어지기 때문에 탐지가 어려움.
- 오픈 소스 기반의 웹쉘 파일들에 대한 분석과 그에 따른 적절한 탐지방안의 적용 및 대응이 필요함.
- 이와 같은 대응 방법을 위해 본 연구에서는 PHP 기반 Apache 웹 서버 Access log와 Yara Library를 활용한 웹쉘 탐지 방법을 적용할 예정임.

2. 과제 수행 방법

- 탐지 방식은 다음과 같이 4가지 과정을 수행함
  - Ⅰ. 테스트 웹 서버에 웹쉘 파일 업로드 및 URL을 통한 서버 명령어를 사용함.
  - Ⅱ. URL 창에 입력된 Apache Access log를 수집하여 텍스트 파일로 저장함. 로그를 수집하는 과정에서 post 방식은 서버에 로그가 자동으로 남지 않기 때문에 오픈 소스를 활용할 예정임.
  - Ⅲ. 수집한 Apache Access log를 대상으로 Yara Library의 규칙을 적용하여 해당하는 URL을 탐지함.
  - Ⅳ. 탐지된 URL을 분석하여 업로드되어있는 파일을 식별한 후 해당 파일의 권한을 조정하여 Root 계정만 사용할 수 있게 변경 후 탐지된 파일을 삭제 혹은 격리 등으로 조치함.
- Yara Library는 파이썬 기반으로 만들어진 라이브러리로서, 악성 파일을 시그니처 기반으로 판별 및 분류할 수 있게 하는 툴이다. Linux, Windows OS에서 모두 사용이 가능하며 소스코드 컴파일, Python 모듈, 파일 실행 방식 등 다양한 방법으로 설치 및 실행이 가능함.
- Apache Access log는 PHP 웹쉘 스크립트를 통해 공격자의 행위에 대한 로그를 파싱하기 위해 PHP Apache 웹 서버 내의 Access log를 활용함.

3. 결과물에 대한 기대효과 및 활용방안

- 웹 서비스를 사용하는 기업 중 웹쉘 솔루션을 도입해서 사용하는 기업은 상대적으로 적음. 또한, 많은 서버를 사용하지 않는 기업의 경우 웹쉘 솔루션을 적용하기에는 비용적인 부분에서 상당한 부담이 될 수 있음. 이와 같은 이유로 웹쉘에 대한 침해 시 탐지가 불가능하

여 침해사고가 발생할 수 있음.

· 본 연구는 Apache 서버를 사용하는 경우 서버에서 탐지 프로세스로 웹쉘 탐지가 가능하므로 비용적 부담 및 침해사고가 줄어들 것으로 예상됨.

4. 수행 일정

주요내용	추진일정				소요 기간(월)
	09	10	11	12	
연구의 기반기술 이론 습득 및 연구 제안서 작성					2주
PHP 기반 Apache 웹 서버 구축					2주
Apache Access log 수집 구현					4주
Yara Library 패턴 구현					4주
탐지 프로그램 GUI 개발					3주
탐지 테스트 및 디버깅					2주

5. 팀원별 역할

No.	성 명	담당 및 수행업무
1	강 * *	연구 기반 학술자료 탐색 및 Yara Library 패턴 구현
2	김 * *	웹쉘 탐지 프로그램 GUI 개발
3	권 * *	Apache Access.log 수집 메소드 구현
4	권 * *	실습용 웹쉘 코드 탐색 및 적용

6. 소요 예산

구분	용도 (과제수행과의 연관성)	품목	규격	단위	수량	단가	금액 (원)
재료비							
그 외	용도 (과제수행의 연관성 기술)			산출 내역			금액 (원)
회의비	과제 수행 팀원과의 회의 진행			주 1회 * 12회			4000원 * 4명
합 계				200,000원			