[별지 제1호 서식] DID 인증기술_Capstone Design 회의록

<table>
<tr><td>동명대학교
TONGMYONG UNIVERSITY</td><td colspan="3">「DID 인증기술_Capstone Design」
회의록</td><td></td></tr>
<tr><td>과제명</td><td colspan="4">Apache Access.log와 Yara Library를 활용한 웹쉘 탐지에 대한 연구</td></tr>
<tr><td>수행기간</td><td colspan="4">2022년 9월 ~ 2022년 12월</td></tr>
<tr><td>회의명</td><td colspan="4">피드백을 통한 캡스톤 디자인 제안서 수정 및 작성</td></tr>
<tr><td>일 시</td><td>2022.09.15.(목)</td><td>팀 명</td><td colspan="2">술래</td></tr>
<tr><td>장 소</td><td>제 1정보통신관</td><td>참석인원</td><td colspan="2">4명</td></tr>
<tr><td>회의내용
(주요사항)</td><td colspan="4">초안으로 작성한 제안서 중 2주차 수업 중 받은 피드백을 중심으로 수정을 진행함.

1) 제목 수정
- 기존 제목은 연구의 방향성과 다르고 다소 포괄적이었음.
- 어떤 방식으로 어떤 연구를 진행할지를 고려해 제목을 수정함.

2) 수행 목적 및 배경 선정 수정
- 애매한 날짜 범위의 표기를 정확한 연, 월로 수정함.
- 수행 목적 표기를 단순한 시그니처 기반에서 좀 더 명확하게 정립함.

3) 과제 수행 방법 수정
- 기존 시그니처 기반 탐지 방법에 대한 정의 대신 Yara Library,
Apache Access log의 활용 방법을 서술함.
- 추가로 가시성을 위해 GUI 프로그램 형태 개발 추가함.

4) 결과물에 대한 기대효과 재정립
- 현재 상용화되어있는 솔루션 오탐 및 미탐에 대한 기대효과는
본 연구와 방향성이 맞지 않는다고 판단하여 삭제함.
- 대기업이 아닌 중소기업 및 자본력이 부족한 회사에서는 솔루션을
자체적으로 도입해서 사용하는 기업이 적음.
- 해당 연구를 통한 결과물을 바탕으로 각종 장비가 아닌 서버 단에서
실행되는 프로세스가 있으면 비용적 부담이 해소 및 침해사고가
줄어들 것으로 예상한다는 결론 도출함.

5) 수행 일정 재정립
1. 연구의 기반기술 이론 습득 및 연구 제안서 작성
2. PHP 기반 Apache 웹 서버 구축
3. Apache Access log 수집 구현
4. Yara Library 패턴 구현
5. 탐지 프로그램 GUI 개발
6. 탐지 테스트 및 디버깅
——</td></tr>
</table>

	서버를 구축하는 작업 진행할 예정 **1) 서버 구축** - 노트북 및 데스크탑, AWS 등 서버 구축 방향 설정 - CentOS, Ubuntu, Red Hat 등 리눅스 서버 결정 **2) 웹 구축** - 서버 구축 후 웹쉘을 업로드 할 수 있는 웹을 구축할 예정 - Apache 웹 서버 구축, PHP 설치 등을 진행 - 여러 오류를 예상해 2회차에는 서버 및 웹 구축까지 진행 예정

위와 같이 회의 결과보고서를 제출합니다.

2022 년 9 월 25 일

소 속 : 정보보호학과

팀 장 : 강 태 화 (서명)

동명대학교 정보보호학과 담당교수 귀하

동명대학교
TONGMYONG UNIVERSITY

「DID 인증기술_Capstone Design」