캡스톤디자인 판넬 제작용

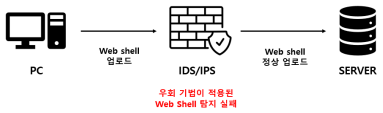
대학/학과	AI융합대학 / 정보보호학과	지도교수	신승수
팀 명	술래	과제유형/번호	D유형/ D6
작 품 명	Yara Library를 활용한 웹쉘 탐지 프로그램		
참여학생	강 * 화, 권 * 빈, 김 * 수, 권 * 헌		
참여기업	-		

과제 목적 및 배경

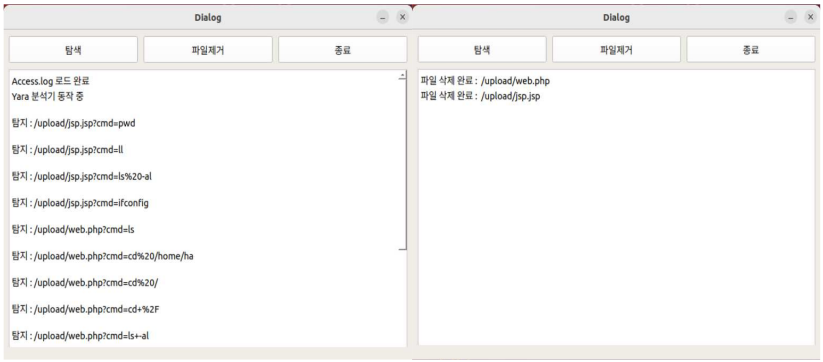
웹의 대중화 시대로 웹 보안에 대한 관심은 필연적으로 고조되고 있다. 또한 보안 위협 중 웹 기반 해킹 공격이 절반 이상의 높은 비중을 차지하며, 그 중 웹쉘을 통한 웹 서버 공격이 주를 이루고 있다. 웹 취약점을 이용하고 다양한 탐지 우회기법이 적용된 웹쉘은 일반적인 서버관리자가 해킹 여부를 확인하기 힘들며, 피해를 인지하더라도 탐지가 어려워 대응의 한계가 명확하다. 따라서 오픈 소스 기반의 웹쉘 파일들에 대한 분석과 그에 따른 적절한 탐지방안의 적용이 필요하다. 그러므로 웹쉘을 탐지하는 솔루션으로는 방화벽이나 백신을 사용하기보다 웹쉘 전용 보안 솔루션을 사용하는 것이 효과적이다.

과제 내용 / 작품 설명

- 방화벽은 한 번 허용된 IP, PORT로 부터 오는 공격을 방어하지 못하고, IDS/IPS는 네트워크 계층에서 동작하여 어플리케이션 계층에서 작동하는 웹쉘을 탐지하기는 어렵다.
- 이를 해결하기 위해 웹 페이지에서 들어오는 모든 정보를 수집하는 접근 로그를 활용하여 웹쉘 실행 로그를 탐지 및 처리한다.
- 수집된 접근 로그들은 정규표현식을 통해 파싱한 후 텍스트 파일로 저장한다. Yara Library를 이용하여 정립된 Yara Rule은 저장된 텍스트파일을 검사하여 웹쉘 실행 유무를 판단한다.



작품 사진



활용 방안 및 기대효과

• 기대효과

- 웹쉘 탐지를 위한 비용 절감 및 내재된 위험 요소 방지

• 활용방안

- 웹 서버 네트워크 장비에서 우회하여 침투한 웹쉘에 대한 탐지 가능
- 네트워크 장비와 같이 사용하여 네트워크 및 어플리케이션 계층의 보안 강화