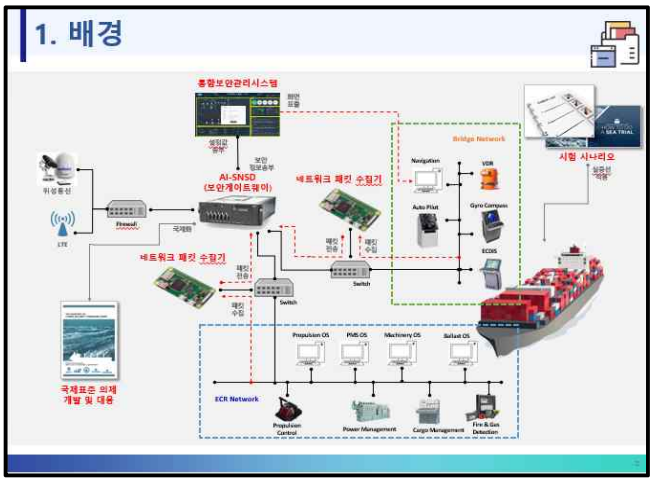
선박사이버보안 침해시험의 이해

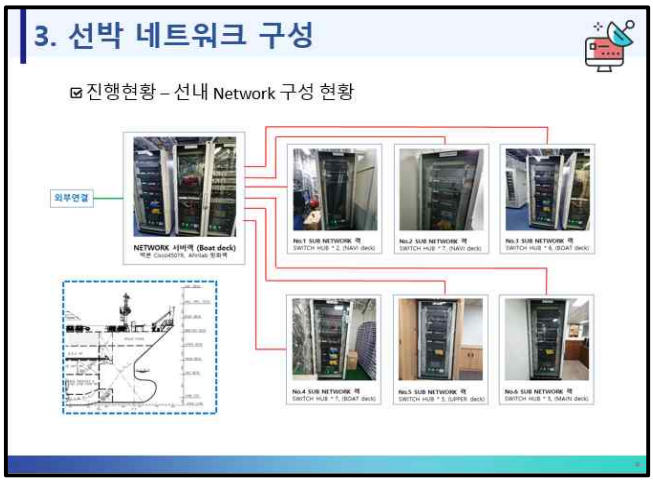
윤경국* · 전현민** · 허재정** · 오세진** · 노정호** · † 김종수

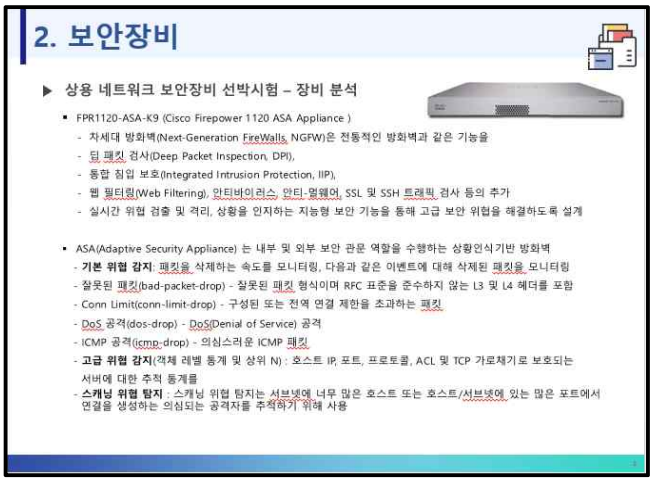
*,**,† 한국해양대학교

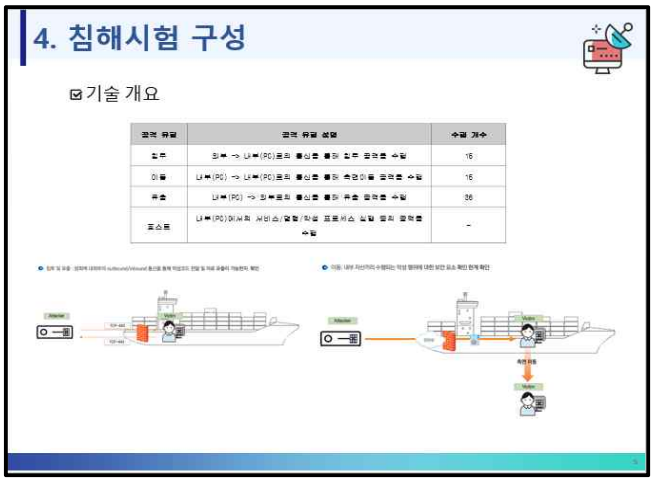
요 약 : 스마트선박 및 자율운항선박에 탑재될 선박 네트워크 보안장비에 대한 모의 공격 방법 및 정보통신망 보안진단 절차에 관하여 이해한다. 선박사이버보안 침해시험을 통하여 보안사고 예방을 통한 선박의 운항 안전성을 확보 하고자 합니다.

핵심용어 : 자율운항선박, 선박사이버보안, 보안장비, 보안진단, 침해시험









† 교신저자 : jongskim@kmou.ac.kr
* 정회원 : kkyoon@kmou.ac.kr

5. BAS 개요

1.4 BAS(Breach and Attack Simulation)

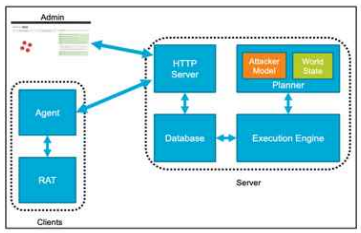
내부의 상황을 자동으로 그리고 가능하면 전체 시스템을 대상으로 기존 서비스에 전혀 해를 가하지 않는 방법으로 실제 해킹 시도가 필요함. 이때 어떤 공격들이 발생할 수 있는지를 알려줄 수 있는 도구도 필요함. 이는 기존에 모의해킹에서 보는 웹사이트의 취약점 하나하나를 찾는 웹취약점 스캐너와는 다른 것이라 하겠다.

구분	지원내용
공격시나리오	• Persistence • Privilege Escalation • Lateral Movement • Access to other Data Stores • C&C • Ex-filtration
주요 기술적 테스트 대상	• Access/Routing /Availability • Data Loss Prevention (DLP) • Content/Web Filtering • Firewall • Network and Host IPS/IDS • AntiVirus (AV) • SIEM • SSL Certificates

6. Caldera 개요

1.5 Caldera

칼데라 (CALDERA)는 MITRE™에서 개발한 APT 시뮬레이터 중 가장 최초이자 잘 알려진 시스템입니다. 2016년부터 관련 연구(논문)가 시작되었고 APT 시뮬레이터 구조를 이해하기 가장 좋은 예제입니다. 하지만 초기 버전인 만큼 MITRE ATT&CK Matrix를 적용하고 있지 않으며, 악성 행위를 하는 RAT이 미리 설치되어 있어 새로운 행위를 적용하려면 수정하기 쉽지 않습니다.



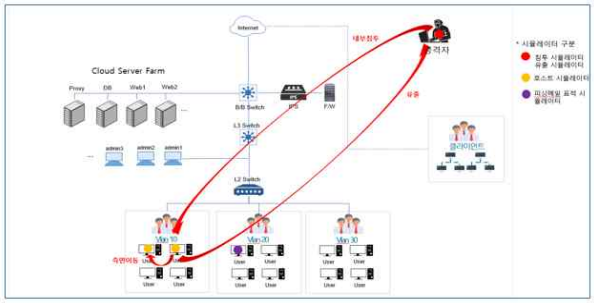
7. APT29

2. APT29 그룹

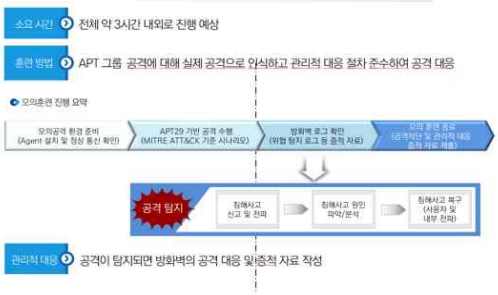
2.1 APT29 그룹 개요

지능형 지속 공격(advanced persistent threat, APT)은 잠행적이고 지속적인 컴퓨터 해킹 프로세스를의 잠행으로, 특정 실체를 목표로 하는 사장이나 사정들에 의해 종종 자휘된다. 지능형 지속 공격은 보통 개인 단체, 국가, 또는 사업체나 정치 단체를 표적으로 삼는다. 이 공격은 오랜 시간 동안 상당한 정도의 은밀함이 요구된다. *고급*(advanced) 프로세스는 시스템 내의 취약점을 공격하기 위해 악성 소프트웨어를 이용한 복잡한 기법을 나타내고 *지속*(persistent) 프로세스는 외부 C&C(커맨드 앤드 컨트롤) 시스템이 지속적으로 특정 대상의 데이터를 감시하고 추출한다. *위협*(threat) 프로세스는 공격을 자휘할 때 인간이 동반됨을 뜻한다.APT29는 러시아의 해킹 그룹으로서 다른 이름으로 코지 베어(Cozy Bear) 혹은 코

8. 시험시나리오



9. 침해시험



10. 침해시험 결과

공격 유형	공격 유형 설명	수행 계수
침투	외부 -> 내부(PC)로의 통신을 통해 침투 공격을 수행	15
이동	내부(PC) -> 내부(PC)로의 통신을 통해 측면이동 공격을 수행	15
유출	내부(PC) -> 외부로의 통신을 통해 유출 공격을 수행	36
호스트	내부(PC)에서의 서비스/명령/의성 프로세스 실행 등의 공격을 수행	-

출발지(Attaker)	목적지(Victim)	포트
211.250.xxx.xxx	Victim IP	TCP:443
Victim IP	211.250.xx	Any