

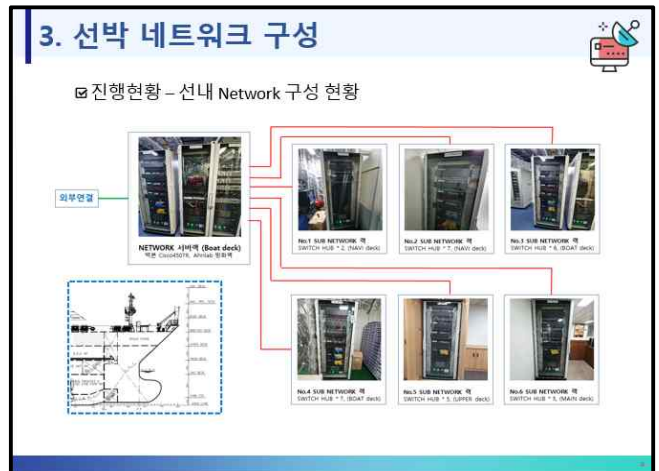
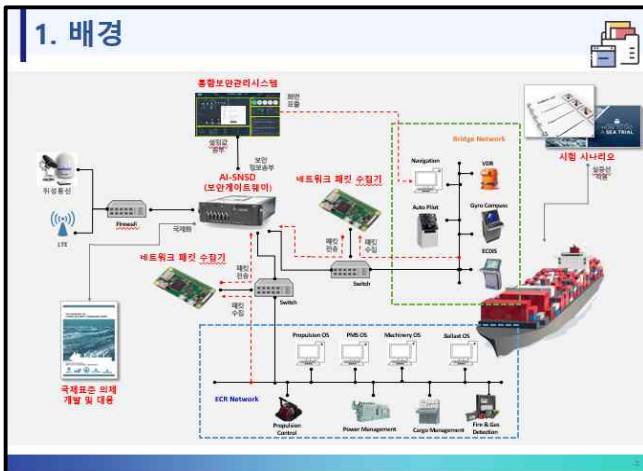
선박사이버보안 침해시험의 이해

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

*,**,† 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 함이다.

핵심용어 : 자율운항선박, 선박사이버보안, 보안장비, 보안진단, 침해시험



2. 보안장비

▶ 상용 네트워크 보안장비 선박시험 - 장비 분석

- FPR1120-ASA-K9 (Cisco Firepower 1120 ASA Appliance)**
 - 차세대 방화벽(Next-Generation FireWalls, NGFW)은 전통적인 방화벽과 같은 기능을
 - 딥 패킷 검사(Dep Packet Inspection, DPI),
 - 통합 침입 보호(Integrated Intrusion Protection, IIP),
 - 웹 필터링(Web Filtering), 안티바이러스, 안티-말웨어, SSL 및 SSH 트래픽 검사 등의 추가
 - 실시간 위협 검출 및 격리, 상황을 인지하는 지능형 보안 기능을 통해 고급 보안 위협을 해결하도록 설계
- ASA(Adaptive Security Appliance)** 는 내부 및 외부 보안 관련 역할을 수행하는 상황인식기반 방화벽
 - 기본 위협 감지**: 패킷을 삭제하는 속도를 모니터링, 다음과 같은 이벤트에 대해 삭제된 패킷을 모니터링
 - 잘못된 패킷(bad-packet-drop) - 잘못된 패킷 형식이며 RFC 표준을 준수하지 않는 L3 및 L4 헤더를 포함
 - Conn Limit(conn-limit-drop) - 구성된 또는 전역 연결 제한을 초과하는 패킷
 - DoS 공격(dos-drop) - DoS(Denial of Service) 공격
 - ICMP 공격(icmp-drop) - 의심스러운 ICMP 패킷
 - 고급 위협 감지**(각체 레벨 통계 및 상위 N) : 호스트 IP, 포트, 프로토콜, ACL 및 TCP 가로제기로 보호되는 서버에 대한 추적 통계를
 - 스캐닝 위협 탐지** : 스캐닝 위협 탐지는 서버넷에 너무 많은 호스트 또는 호스트/서버넷에 있는 많은 포트에서 연결을 생성하는 의심되는 공격자를 추적하기 위해 사용

4. 침해시험 구성

☑ 기술 개요

공격 방법	공격 유형 설명	수행 개수
접근	외부 → 내부 (PC)로 통신을 통한 접근 권한 수립	16
이동	내부 (PC) → 내부 (PC)로 통신을 통한 권한 이동 및 공격권 수립	16
유출	내부 (PC) → 외부 (PC)로 통신을 통한 유출 공격권 수립	20
도소통	내부 (PC)와 외부 (서버넷/클라우드)로 통신을 통한 도소통 공격권 수립	-

† 교신저자 : jongskim@kmou.ac.kr

* 정회원 : kkyoon@kmou.ac.kr

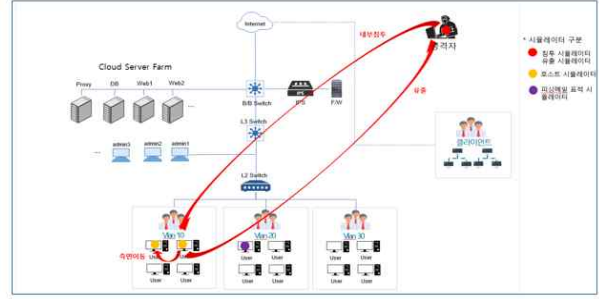
5. BAS 개요

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 필요한 이때 어떤 공격들이 발생할 수 있는지를 알려줄 수 있는 도구도 필요하다. 이는 기존에 모의해킹에서 보는 웹사이트의 취약점 하나하나를 찾는 웹 취약점 스캐너와는 다른 것이다 하겠다.

구분	지원내용	기술적 테스트 대상
공격시나리오	<ul style="list-style-type: none"> Persistence Privilege Escalation Lateral Movement Access to other Data Stores C&C Ex-filtration 	<ul style="list-style-type: none"> Active Directory Microsoft Exchange Microsoft SQL Server Microsoft SharePoint Microsoft Dynamics CRM Microsoft Lync Microsoft Teams Microsoft Word Microsoft PowerPoint Microsoft Excel Microsoft Access Microsoft Outlook Microsoft OneDrive Microsoft Teams Microsoft SharePoint Microsoft Dynamics CRM Microsoft Lync Microsoft Teams Microsoft Word Microsoft PowerPoint Microsoft Excel Microsoft Access Microsoft Outlook Microsoft OneDrive
주요 기술적 테스트 대상	<ul style="list-style-type: none"> Access/Routing /Availability Data Loss Prevention (DLP) Content/Web Filtering Firewall Network and Host IPS/IDS AntiVirus (AV) SIEM SSL Certificates 	<ul style="list-style-type: none"> Microsoft Exchange Microsoft SQL Server Microsoft SharePoint Microsoft Dynamics CRM Microsoft Lync Microsoft Teams Microsoft Word Microsoft PowerPoint Microsoft Excel Microsoft Access Microsoft Outlook Microsoft OneDrive

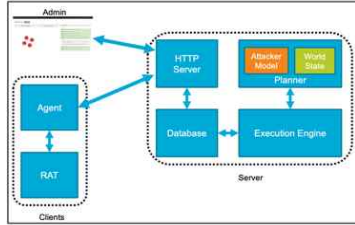
8. 시험시나리오



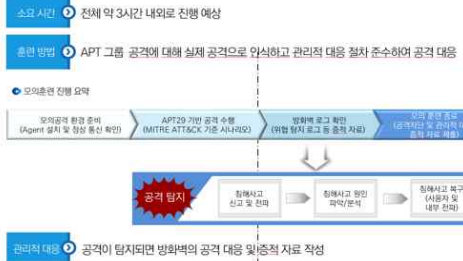
6. Caldera 개요

1.5 Caldera

칼데라 (CALDERA)는 MITRE™에서 개발한 APT 시나리오를 가장 최적으로 잘 알려진 시나리오이다. 2016년부터 관련 연구(논문)가 시작되었고 APT 시나리오의 구조를 이해하기 가장 좋은 예제입니다. 하지만 초기 버전인 MITRE ATT&CK Matrix를 적용하고 있지 않으며, 악성 행위를 하는 RAT이 미리 설치되어 있어 새로운 행위를 적용하려면 수정이 필요합니다.



9. 침해시험



7. APT29

2. APT29 그룹

2.1 APT29 그룹 개요

지능형 지속 공격(advanced persistent threat, APT)은 침범적이고 지속적인 컴퓨터 해킹 프로세스들의 집합으로, 특정 실체를 목표로 하는 사냥이나 사냥물에 의해 종종 지칭된다. 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 지휘할 때 인건이 증발됨을 뜻한다.APT29는 러시아의 해킹 그룹으로서 다른 이름으로 코지 베어(Cozy Bear) 혹은 코

2.4 APT29 공격시나리오 SCORPION



10. 침해시험 결과

공격 유형	공격 유형 설명	수행 개수
입부	외부 -> 내부(PC)로의 통신을 통해 입부 공격을 수행	15
미들	내부(PC) -> 내부(PC)로의 통신을 통해 측면미들 공격을 수행	15
유출	내부(PC) -> 외부로의 통신을 통해 유출 공격을 수행	36
호스트	내부(PC)에서의 서비스생성/서정 프로세스 실행 등의 공격을 수행	-



공격자(Attacker)	목표지(Victim)	포트
211.250.xxx	Victim 코	TCP-443
Victim 코	211.250.xxx	Any