

과제 개요

배경 및 목표

- 기업 및 기관의 클라우드 마이그레이션이 증가함에 따라 클라우드 보안의 중요성이 강조됨
- 클라우드 환경의 보안을 강화하기 위해 MITRE ATT&CK 프레임워크를 기반으로 보안 공격 자동화 플랫폼 개발
- 해당 플랫폼은 대상 시스템의 취약점을 이용하여 시스템을 공격한 후 사용자에게 그 결과를 알려주어 보안을 강화할 수 있도록 도움
- 공격 자동화를 통해 사용자가 클라우드 환경에 대한 사전 지식 없이 보안 검사가 가능함

과제 내용

공격 시나리오 생성

- 공격 대상 시스템에서 특정 목표를 달성하기 위한 일련의 과정을 '공격 시나리오'라고 정의
- 공격 시나리오는 MITRE ATT&CK 프레임워크의 Technique으로 구성

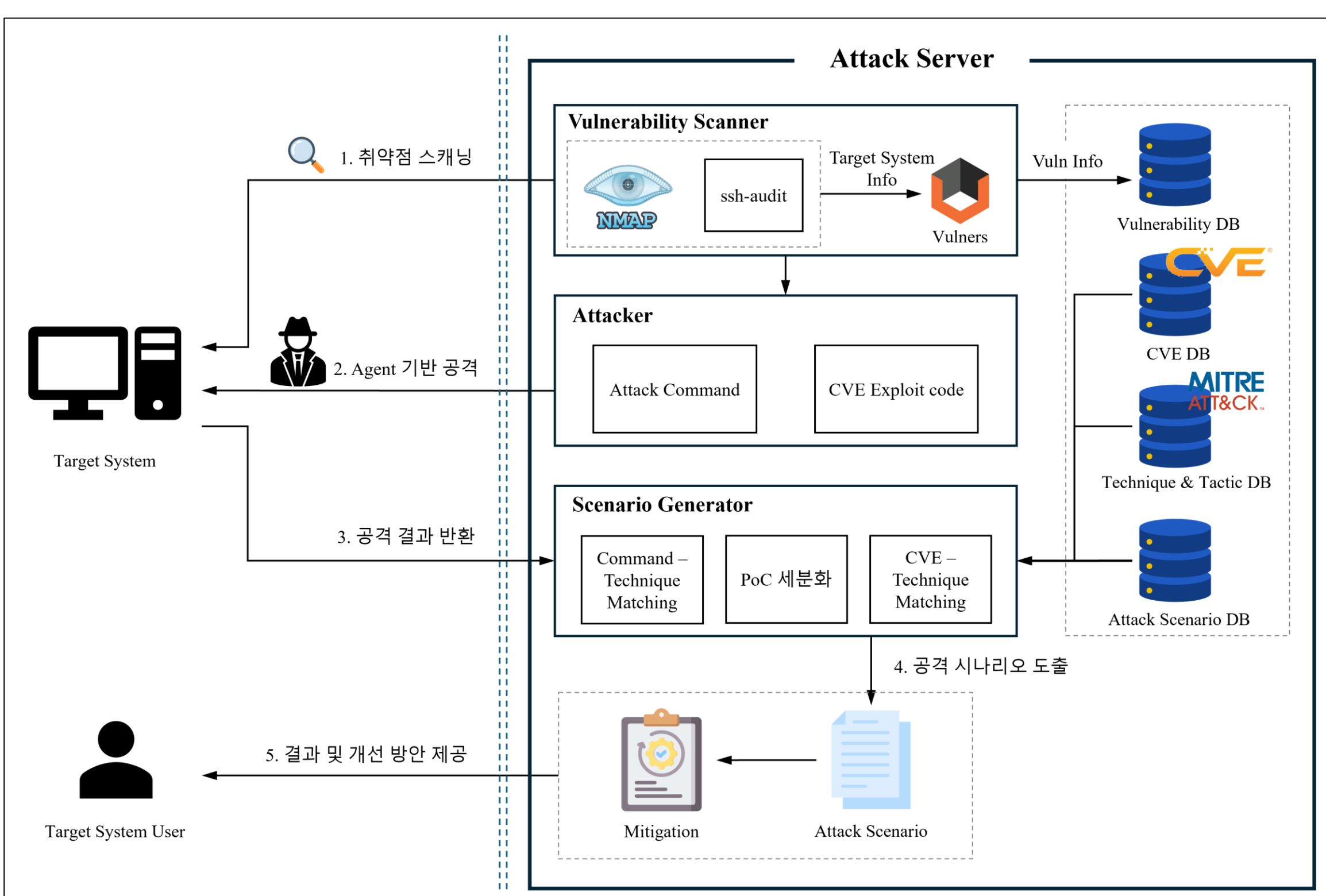
MITRE ATT&CK 기반 침투 테스트

- MITRE ATT&CK 프레임워크에서 정의한 공격 기법들을 구현하고 그 기법들을 연결하여 공격 시나리오 구현
- Agent를 이용하여 대상 시스템을 공격하고 그 결과 값을 기반으로 시스템을 공격할 수 있는 시나리오 도출

CVE Exploit 기반 침투 테스트

- CVE(Common Vulnerabilities and Exposures)의 알려진 PoC의 동작 흐름과 MITRE ATT&CK의 Technique과 매핑하여 공격 시나리오 구성
- 대상 시스템의 IP 주소 혹은 Agent를 이용하여 해당 시스템에서 발견된 CVE 목록과 Exploit 성공한 CVE를 출력

Service Architecture



결과

MITRE ATT&CK

ATTACK SCENARIO: Steal Sensitive File		
Collection	Exfiltration	
Data from Local System	Archive Collected Data Archive via Utility	
Data Staged Local Data Staging	Exfiltration Over C2 Channel	
VIEW DETAIL		
ATTACK SCENARIO: WIFI DOS		
Privilege Escalation	Discovery	Impact
Abuse Elevation Control Mechanism: Bypass User Access Control	System Network Configuration Discovery	Endpoint Denial of Service
VIEW DETAIL		
ATTACK SCENARIO: Change User Password		
Privilege Escalation	Discovery	Impact
Abuse Elevation Control Mechanism: Bypass User Access Control	System Owner/User Discovery	Account Access Removal
VIEW DETAIL		

CVE ATTACK

IP Address: 192.168.29.132	
CVE LIST	
Service : ssh - 22	
CVE-2024-21195 Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Layout Templates). Supported versions that are affected are 7.0.0.0, 7.6.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:CAU/C:H/L:N/AE). https://vulners.com/cve/CVE-2024-21195	
CVE-2024-21191 Vulnerability in the Oracle Enterprise Manager Fusion Middleware Control product of Oracle Fusion Middleware (component: FMW Control PlugIn). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Manager Fusion Middleware Control. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Manager Fusion Middleware Control accessible data as well as unauthorized update, insert or delete access to some of Oracle Enterprise Manager Fusion Middleware Control accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:CAU/C:H/L:N/AE). https://vulners.com/cve/CVE-2024-21191	
CVE-2024-21689 This High severity RCE (Remote Code Execution) vulnerability CVE-2024-21689 was introduced in versions 9.1.0, 9.2.0, 9.3.0, 9.4.0, 9.5.0, and 9.6.0 of Bamboo Data Center and Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 7.6, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Bamboo Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Bamboo Data Center and Server 9.2.1 Upgrade to a release greater than or equal to 9.2.1 Bamboo Data Center and Server 9.6 Upgrade to a release greater than or equal to 9.6.5 See the release notes (https://confluence.atlassian.com/bambooreleases/bamboo-release-notes-118973865.html). You can download the latest version of Bamboo Data Center and Server from the download center (https://www.atlassian.com/software/Bamboo/download-archives). This vulnerability was reported via our Bug Bounty program. https://vulners.com/cve/CVE-2024-21689	
CVE-2024-38029 Microsoft OpenSSH for Windows Remote Execution Vulnerability https://vulners.com/cve/CVE-2024-38029	
CVE-2024-43615 Microsoft OpenSSH for Windows Remote Execution Vulnerability https://vulners.com/cve/CVE-2024-43615	