

PoC 구현을 통한 클라우드 보안 공격 자동화 도구 개발

201824441 김승혁

201824507 송재홍

202145827 정재영

연구 배경

▪ MITRE ATT&CK 프레임워크

- 사이버 공격 기술과 방어 방법을 체계적으로 정리한 지식 기반 (Knowledge Base)

❖ 지식 기반: 모든 정보 또는 지식을 저장, 조직화하고 고객, 직원 및 파트너와 공유할 수 있는 저장소

- 공격 방법(Tactic)과 기술(Technique)을 분석하여 다양한 해킹 기법을 문서화하고 분류한 프레임워크



Tactic

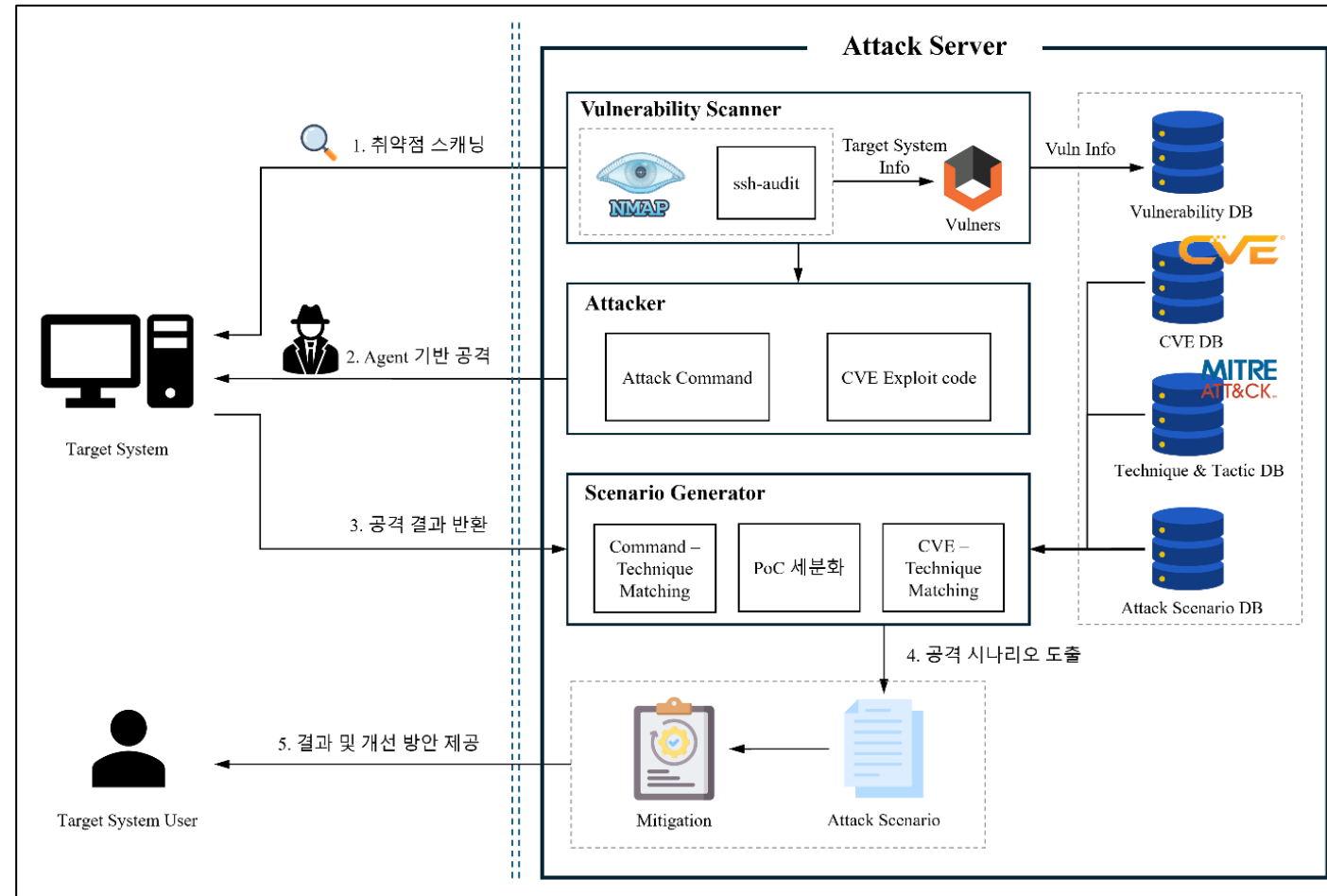
Technique

ATT&CK Matrix for Enterprise			
layout: side ▾ show sub-techniques hide sub-techniques			
Privilege Escalation	Defense Evasion	Credential Access	Discovery
14 techniques	43 techniques	17 techniques	32 techniques
Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)
Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery
Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery
Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard
Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery
Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery
Escape to Host	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery
Event Triggered Execution (16)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion
Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery
Hijack Execution Flow (13)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery
Process Injection (12)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery
Scheduled Task/Job (3)	Hide Artifacts (12)	Steal Application Access Token	Group Policy Discovery
Valid Accounts (4)	Hijack Execution Flow (13)	Steal or Forge Authentication	Log Enumeration
	Impair Defenses (11)		Network Service Discovery
	Impersonation		Network Share Discovery
	Indicator Removal (9)		Network Sniffing
			Password Policy Discovery
			Peripheral Device Discovery

Examples of Tactic & Technique in MITRE ATT&CK Matrix

연구 내용

■ 전체 시스템 구상도



Architecture

연구 내용

■ 공격 시나리오 설계

- MITRE ATT&CK의 Technique과 그에 해당하는 CMD 명령어를 매핑하여 시나리오 설계
- CVE (Common Vulnerabilities and Exposures) PoC의 흐름과 MITRE ATT&CK의 Technique과 매핑하여 시나리오 설계
- 설계한 시나리오를 기반으로 자동화된 침투 테스트 기능 구현
 - MITRE ATT&CK 기반 침투 테스트
 - CVE Exploit 기반 침투 테스트

◆ CVE-2022-0847 (Dirty Pipe)

– MITRE ATT&CK 매트릭스와 매핑

- T1106 - Native API (Execution)**
 - 공격을 수행하기 위해 native OS API 와 상호작용
 - splice, write, pipe, open, fstat 등의 리눅스 시스템 호출
- T1068: Exploitation for Privilege Escalation (Privilege Escalation)**
 - 공격자는 권한을 상승시키기 위해 소프트웨어 취약점을 악용
 - /etc/passwd 파일을 덮어쓰고 이를 통해 시스템의 루트 계정 비밀번호를 설정하여 루트 권한을 획득
- T1548: Abuse Elevation Control Mechanism (Privilege Escalation, Defense Evasion)**
 - 공격자는 더 높은 권한을 얻기 위해 권한 상승을 제어하도록 설계된 메커니즘 우회
 - /etc/passwd 파일을 수정하여 시스템의 사용자 계정을 수정하여 권한을 상승
- T1070: Indicator Removal (Defense Evasion)**
 - 공격자가 자신의 흔적을 지우기 위해 시스템 내에 생성했던 artifact를 삭제 또는 수정
 - /etc/passwd 파일의 원본을 /tmp/passwd.bak에 백업하고 공격 수행 후 원본 파일 복구
- T1005: Data from Local System (Collection)**
 - 취약한 데이터를 찾기 위해 로컬 시스템 자원을 검색
- T1556: Modify Authentication Process (Credential Access, Defense Evasion, Persistence)**
 - 인증 메커니즘 및 사용자의 자격 증명 접근 과정 수정

CVE 2022-0847의 PoC 분석

Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Cloud Administration Command	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/5)	Abuse Elevation Control Mechanism (0/5)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services (0/3)	Adversary-in-the-Middle (0/3)
Command and Scripting Interpreter (0/10)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)
Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/5)	Build Image on Host	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/14)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection
Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (0/4)	Browser Session Hijacking
Inter-Process Communication (0/3)	Compromise Host Software Binary	Boot or Logon Initialization Scripts (0/5)	Deploy Container	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Replication Through Removable Media	Clipboard Data
Native API (0/13)	Create Account (0/3)	Create or Modify System Process (0/5)	Direct Volume Access	Input Capture (0/4)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage
Scheduled Task/Job (0/5)	Create or Modify System Process (0/5)	Domain or Tenant Policy Modification (0/2)	Domain or Tenant Policy Modification (0/2)	Modify Authentication Process (0/3)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (0/2)
Serverless Execution	Event Triggered Execution (0/10)	Escape to Host	Execution Guardrails (0/1)	Multi-Factor Authentication Interception	Device Driver Discovery	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)
Shared Modules	External Remote Services	Event Triggered Execution (0/16)	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Domain Trust Discovery	File and Directory Discovery	Data from Local System (0/3)
Software Deployment Tools	Hijack Execution Flow (0/13)	Exploitation for Privilege Escalation (0/13)	File and Directory Permissions Modification (0/2)	Network Sniffing	File Enumeration	Group Policy Discovery	Data from Network Shared Drive
System Services (0/2)	Implant Internal Image	Hijack Execution Flow (0/13)	Hide Artifacts (0/12)	OS Credential Dumping	Log Enumeration	Network Service Discovery	Data from Removable Media
User Execution (0/3)	Modify Authentication Process (0/5)	Process Injection (0/12)	Hijack Execution Flow (0/13)	Steal Application Access Token	Network Share Discovery	Network Sniffing	Data Staged (0/2)
Windows Management Instrumentation	Office Application Startup (0/6)	Scheduled Task/Job (0/5)	Impersonation (0/11)	Steal or Forge Authentication Certificates	Network Sniffing	Password Policy Discovery	Email Collection (0/3)
	Power Settings	Valid Accounts (0/4)	Indicator Removal (0/3)	Steal or Forge Kerberos Tickets (0/4)	Peripheral Device Discovery	Permission Groups Discovery (0/3)	Input Capture (0/4)
	Pre-OS Boot (0/5)		Indirect Command Execution	Steal Web Session Cookie	Process Discovery	Screen Capture	Video Capture
	Scheduled Task/Job (0/5)		Masquerading (0/9)		Query Registry		
	Server Software Component (0/1)		Modify Authentication Process (0/3)				

CVE 2022-0847의 PoC와 매핑된 Technique

연구 내용

■ 침투 테스트

1. MITRE ATT&CK 기반 침투 테스트

- ① MITRE ATT&CK 기반으로 모의 해킹을 수행
- ② 성공한 공격 시나리오에 대한 결과 및 Mitigation 제공

2. CVE(Common Vulnerabilities and Exposures) Exploit 기반 침투 테스트

ATT&CK Based Penetration Test												
<div>DESKTOP-M40JFDP</div> <div>ATTACK</div>												
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
No techniques available	No techniques available	No techniques available	No techniques available	No techniques available	Abuse Elevation Control Mechanism System User Access Control	Indicator Removal on Host Clear Command History	Process Injection Portable Executable Injection	Process Discovery System Owner/User Discovery Remote System Discovery System Network Configuration Discovery	No techniques available	Data Staged: Local Data Staging Data from Local System	No techniques available	Exfiltration Over C2 Channel Archive Collected Data Archive via Utility
												Endpoint Denial of Service

시스템에 대한 침투 테스트 수행 결과 화면

HOSTNAME: DESKTOP-M40JFDP

ATTACK SCENARIO: WIFI DOS

Privilege Escalation

Abuse Elevation Control Mechanism: Bypass User Access Control

Impact

Endpoint Denial of Service

VIEW DETAIL

Attack Scenario Detail

공격자가 피해자의 WIFI 연결을 끊는 공격 시나리오

공격 순서 및 방어책

Attack 1: Bypass UAC With Akagi64.exe

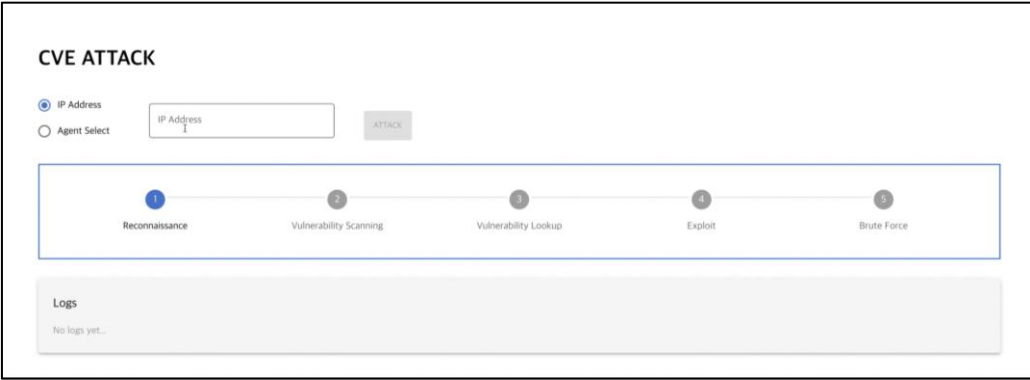
Mitigation

사용된 Command

성공한 공격 시나리오 및 완화 방법 제시 화면

연구 내용

- 침투 테스트
 - 1. MITRE ATT&CK 기반 침투 테스트
 - 2. CVE(Common Vulnerabilities and Exposures) Exploit 기반 침투 테스트
 - ① 대상 시스템에 대한 CVE 탐색
 - ② Exploit으로 연결될 수 있다면 공격을 수행
 - ③ 각 CVE에 대한 MITRE ATT&CK의 Technique과 매핑한 결과 제공
 - ④ Cloud RMF의 CVE ATTACK과의 차이점
 - Cloud RMF에서는 CVE 목록을 출력하고 공격은 수행하지 않음
 - 해당 플랫폼에서는 CVE 목록을 탐색한 이후 시스템 공격 시도



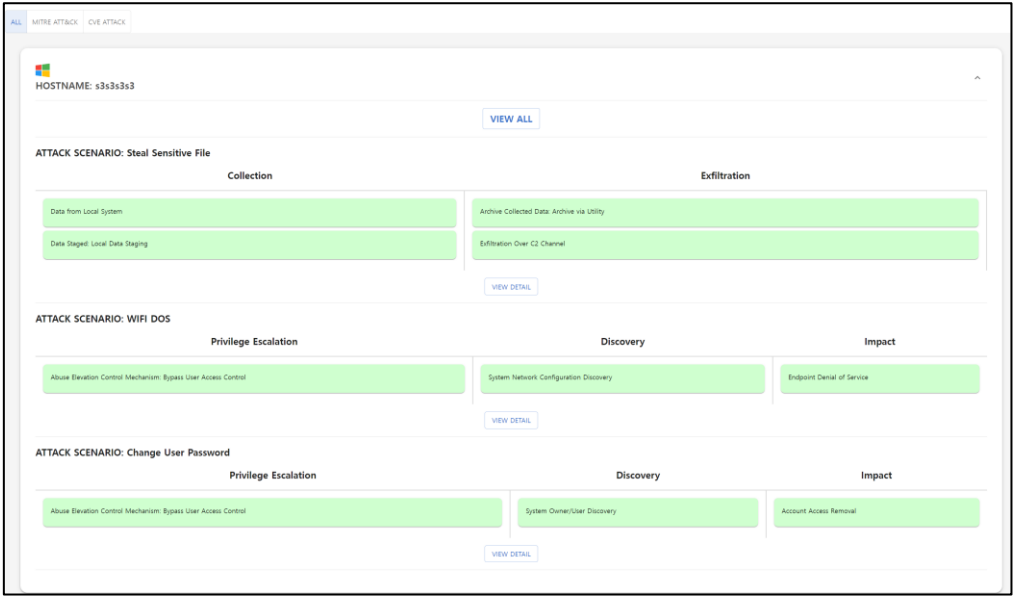
CVE ATTACK 초기 화면

CVE List		
CVE ID	Used Technique	Mitigation
CVE 2024-1086	T1068	If you are using Linux kernel version 3.15 ~ 6.1.76 / 6.2 ~ 6.6.15 / 6.7 ~ 6.7.3, update the kernel to the latest version
	T1543	
	T1547	
	T1059	
	T1203	
CVE 2021-44228	T1190	Log4j 2.15.0 has been released to address the vulnerability
	T1059	
	T1203	
	T1068	
	T1105	
	T1071	

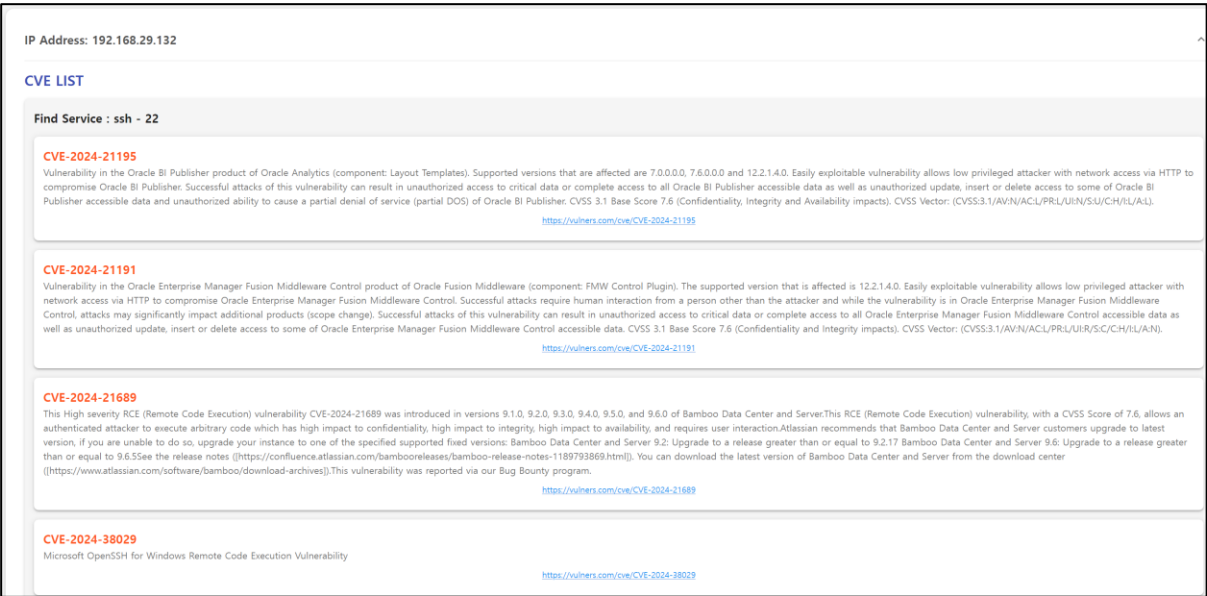
해당 시스템 대상 CVE 리스트 출력

연구 내용

- 침투 테스트 – 결과
 - 대상 시스템에 수행된 공격 결과와 이에 대응하는 완화 방법 출력
 - 관련 CVE 목록 출력



결과 화면



해당 시스템 대상 CVE 리스트 출력

감사합니다
