2024 전기 졸업과제 착수보고서

PoC 구현을 통한 클라우드 보안 공격 자동화 도구 개발

지도 교수 : 최윤호

팀 명 : 417호

팀 원 : 201824441 김승혁

201824507 송재홍

202145827 정재영

목차

1. 프로젝트 개요

1.1 배경 및 필요성

최근 클라우드 기술의 발전으로 기업들은 기존의 on-premise 시스템에서 클라우드 환경으로의 전환을 가속화하고 있다. 클라우드는 유연성과 확장성, 비용 효율성 등의 이점을 제공하지만, 동시에 새로운 보안 위협을 초래하기도 한다. 클라우드 환경에서의 보안 문제는 계속해서 증가하고 있으며, 이는 클라우드 서비스 제공업체와 클라우드 사용자 모두에게 중요한 과제로 대두되고 있다. 특히, 클라우드 인프라를 겨냥한 사이버 공격은 점점 더 정교해지고 있으며, 그 파급력도 커지고 있다. 이에 따라 클라우드 보안에 대한 심층적인 연구와 적절한 대응이 필요하다.

클라우드 환경에서는 전통적인 보안 모델이 충분하지 않기 때문에, 새로운 보안 전략과 도구가 요구된다. 특히, CVE(공개된 취약점)와 Mitre Att&ck 프레임워크를 기반으로 한 공격 시나리오는 클라우드 보안의 주요 위협 요소로 떠오르고 있다. 이러한 공격들을 사전에 탐지하고 방어하기 위해서는 공격 기법을 이해하고, 이를 시뮬레이션할 수 있는 PoC(Proof of Concept)를 구현하는 것이 중요하다. 이를 통해 클라우드 환경에서의 취약점 wsl을 실질적으로 확인하고, 개선 방안을 도출할 수 있다.

1.2 과제 목표 및 기대효과

본 과제의 목표는 클라우드 보안을 강화하기 위해 Mitre Att&ck 기반으로 PoC(Proof of Concept) 구현을 통한 클라우드 보안 공격 자동화 도구를 개발하는 것이다. 구체적으로, 클라우드 환경에서 발생할 수 있는 다양한 보안 취약점과 공격 기법을 분석하고, 등록된 CVE를 분석하여 클라우드 등의 취약점을 파악한다.

그에 따른 공격 시나리오를 설계하는 것으로 자동화 도구로 구현하는 것을 목표로 한다. 이를 통해 기대할 수 있는 효과는 다음과 같다:

1. **공격 탐지 및 대응 능력 향상**: 다양한 클라우드 보안 공격 시나리오를 자동으로 수행하고 탐지할 수 있는 도구를 개발함으로써, 클라우드 환경에서의 보안 사고에 대한 대응 능력을 크게 향상시킬 수 있다. 이는 보안 팀이 실시간으로 위협을 모니터링하고, 신속하게 대응할 수 있도록 도와준다.

2. **보안 취약점 식별 및 개선**: 자동화된 도구를 통해 클라우드 환경의 취약점을 사전에 발견하고, 이를 보완하는 과정을 통해 보안 수준을 전반적으로 향상시킬 수 있다. 이는 클라우드 인프라의 안전성을 높이고, 잠재적인 보안 사고를 예방하는 데 기여할 것이다.

3. **보안 교육 및 인식 제고**: 개발된 도구를 활용하여 보안 교육과 훈련을 실시함으로써, 클라우드 보안에 대한 인식을 제고하고, 관련 지식을 실무에 적용할 수 있는 기회를 제공할 수 있다. 이는 보안 문화 정착과 보안 사고 대응 역량 강화에 도움이 된다.

4. **표준화된 보안 테스트 환경 제공**: PoC를 통해 구현된 공격 시나리오는 표준화된 보안 테스트 환경을 제공하여, 다양한 클라우드 서비스 및 애플리케이션에 대한 보안 검증을 체계적으로 수행할 수 있도록 한다. 이는 보안 검증 단계를 더욱 효율적으로 관리하는 데 기여할 것이다.

2. 진행 방안

본 과제는 클라우드 보안 공격에 대한 심층적인 분석과 이를 기반으로 한 자동화 도구 개발을 목표로 한다. 이를 위해 다음과 같은 단계별 진행 방안을 수립하였다.

2.1 클라우드 관련 보안 공격 분석

최신 클라우드 관련 보안 공격 기법과 취약점을 체계적으로 분석한다. 이를 위해 CVE Database, MITRE ATT&CK 프레임워크, 보안 연구 자료 등을 참고하여 다양한 공격 벡터와 사례를 조사한다. 주요 활동은 다음과 같다.

- **MITRE ATT&CK 분석**: MITRE ATT&CK 프레임워크에서 클라우드 환경과 관련된 공격 기법(TTPs)을 추출하고, 이를 심층적으로 분석한다.

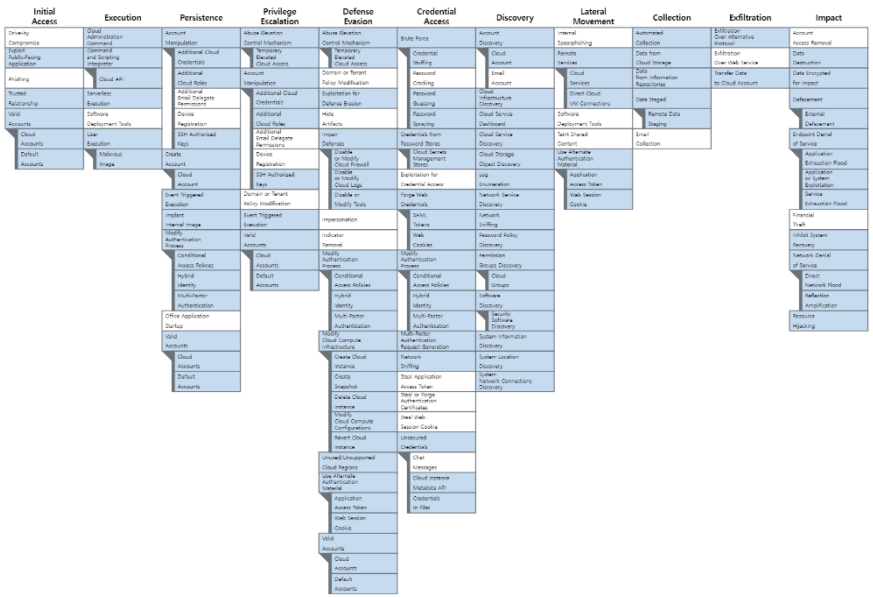

그림 1. IaaS 관련 Techniques (Mitre Att&ck Navigator)

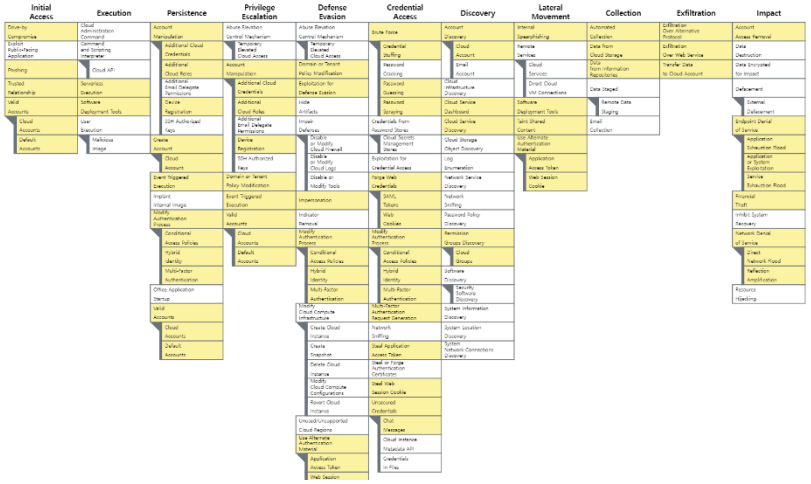

그림 2. SaaS 관련 Techniques (Mitre Att&ck Navigator)

- **CVE 목록 작성**: 클라우드 환경에서 흔히 발생하는 취약점들을 조사하고, 관련 CVE 목록을 작성한다.

- **사례 연구**: 최근 발생한 클라우드 보안 사고 사례를 연구하여 공격자들이 사용한 기법과 취약점을 파악한다.

Category	Built-in Windows Command	Cobalt Strike	Metasploit	Description
Discovery				
T1082	ver	shell ver		Get the Windows OS version that's running
T1082	set	shell set	get_env.rb	Print all of the environment variables
T1033	whoami /all /fo list	shell whoami /all /fo list	getuid	Get current user information, SID, domain, groups the user belongs to, security privs of the user
T1082	net config workstation net config server	shell net config workstation shell net config server		Get computer name, username, OS software version, domain information, DNS, logon domain
T1016	ipconfig /all	shell ipconfig	ipconfig post/windows/gather/enum_domains	Get information about the domain, network adapters, DNS / WSUS servers
T1082	systeminfo [/s COMPNAME] [/u DOMAIN\user] [/p password]	systemprofiler tool if no access yet (victim browses to website) or shell systeminfo (if you already have a beacon)	sysinfo, run winenum, get_env.rb	Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties, such as RAM, disk space, and network cards
T1012	reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections	shell reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections	reg queryval -k "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" -v fDenyTSConnections post/windows/gather/enum_termserv	Check for the current registry value for terminal services, if it's 0, then terminal services are enabled. If it's 1, then they're disabled
T1016	arp -a route print	shell arp -a	route	Display the ARP table
T1049	netstat -ano[b]	shell c:\windows\sysnative\netstat.exe -ano[b]	post/windows/gather/tcpnetstat	Display current TCP/IP network connections (b requires elevated privs so you can see the process that opened the connection)
T1057	tasklist /v [/svc] net start qprocess *	ps shell tasklist /v [/svc] shell net start	ps post/windows/gather/enum_services	Display list of currently running processes and services on the system
T1069	net localgroup "Administrators"	shell net localgroup "Administrators"	post/windows/gather/local_admin_search_enum	Display the list of local administrator accounts on the workstation
T1069	net group ["Domain Admins"] /domain[:DOMAIN]	net group ["Domain Admins"] /domain	domain_list_gen.rb post/windows/gather/enum_domain_group_users	Display the list of domain administrator accounts
T1087	net user [username] [/domain]	shell net user [username] [/domain]	post/windows/gather/enum_ad_users auxiliary/scanner/smb/smb_enumusers	Used to add, delete, and manage the users on the computer. Run this command on the users discovered from the previous two commands to gather more information on targeted users.
T1018	net group "Domain Computers" /domain[:DOMAIN]	net group "Domain Computers" /domain	post/windows/gather/enum_ad_computers post/windows/gather/enum_computers	Display the list of domain computers in the domain by showing their computer accounts (COMP_NAME$)
T1018	net group "Domain Controllers" /domain[:DOMAIN]	net group "Domain Controllers" /domain		Display the list of domain controllers in the network
T1077	net use [\\ip\path] [password] [/user:DOMAIN\user] net use \\COMP\ADMIN$ password /user:COMP\Administrator (checking password reuse on local admin account)	shell net use [\\ip\path] [password] [/user:DOMAIN\user]		Used to view network shared resource information, add a new network resource, and remove an old network resource from the computer. Run this against computers discovered from the previous two commands to view the shares that are available on them.
T1016	nbtstat -a (IP | COMP_NAME)	shell c:\windows\sysnative\nbtstat.exe -a (IP | COMP_NAME)		Used to get the MAC and IP addresses as well as some descriptive codes for machines (0x1C indicates a domain controller)
T1135	net share	net share	auxiliary/scanner/smb/smb_enumshares	Used to view network shared resource information, share a new network resource, and remove an old shared network resource from the workstation. Not for remote queries
T1049	net session | find / "\\"	shell net session | find / "\\"	post/windows/gather/enum_logged_on_users	Display the list of active SMB sessions on the workstation so you can see which users have active connections.
T1135	net view \\host /all [/domain:domain]	net view \\host /domain	auxiliary/scanner/smb/smb_enumshares	Display the list of workstations and network devices on the network.
T1018	nltest /dclist[:domain]			Display the trust relationship between the workstation and the domain - must be elevated to use this!
T1053	schtasks [/s HOSTNAME]	shell schtasks		Displays all of the currently scheduled tasks to be run on a computer
T1018	echo %LOGONSERVER%	shell echo %LOGONSERVER%		Display the active directory login server of the workstation
T1087	dsquery group "ou=Domain Admins,dc=domain,dc=com" dsquery user "dc=domain,dc=com" dsquery * OU="Domain Admins",DC=domain,DC=com -scope base -attr SAMAccountName userPrincipalName Description dsquery * -filter "(&(objectCategory=contact)(objectCategory=person)(mail=*)(objectClass=user))" -Attr samAccountName mail -Limit 0 dsquery * -filter "(&(objectCategory=group)(name="Admin"))" -Attr name description members	shell dsquery group "ou=Domain Admins",dc=domain,dc=com" shell dsquery user "dc=domain,dc=com" shell dsquery * OU="Domain Admins",dc=domain,dc=com -scope base -attr SAMAccountName userPrincipleName Description shell dsquery * -filter "(&(objectCategory=contact)(objectCategory=person)(mail=*)(objectClass=user))" -Attr samAccountName mail -Limit 0 shell dsquery * -filter "(&(objectCategory=group)(name="Admin"))" -Attr name description members		Dsquery is a Windows utility on servers that facilitates querying the Active Directory of the domain for lots of information about users, groups, and permissions. When constructing dsquery commands, if your domain is "subdomain.domain.tld", then your query will include "dc=subdomain,dc=domain,dc=tld"

그림 3. APT3 공격 사례에서 사용된 Technique 별 windows cmd, Cobalt Strike, Metasploit 명령어 정리 표 (Mitre Att&ck 제공)

- **클라우드 구성 요소 분석**: IaaS, SaaS 외에도 클라우드를 구성하는 요소들(ex. Hypervisor)의 취약점을 분석하여 다양한 방면으로 공격 사례 및 취약점 등을 분석한다.

2.2 공격 시나리오 설계

분석된 공격 기법과 취약점을 바탕으로, 구체적인 공격 시나리오를 설계한다. 이 단계에서는 클라우드 환경에서 재현 가능한 PoC 를 설계하여, 공격 상황을 시뮬레이션할 수 있도록 한다. 주요 활동은 다음과 같다:

- **공격 목표 설정**: Mitre Att&ck 의 TTPs 를 기반으로 공격 목표(Tactic)를 설정하고, 이를 이루기 위한 Techniques 를 구현한다. 이를 위해 그림 3. 에서와 같이 Technique 별 명령어를

- **시나리오 순서화**: Mitre Att&ck 에서 제공하는 Navigator 를 통해 왼쪽에서 오른쪽(목표 Tactic)으로 가는 흐름으로 공격 시나리오를 순서화한다.

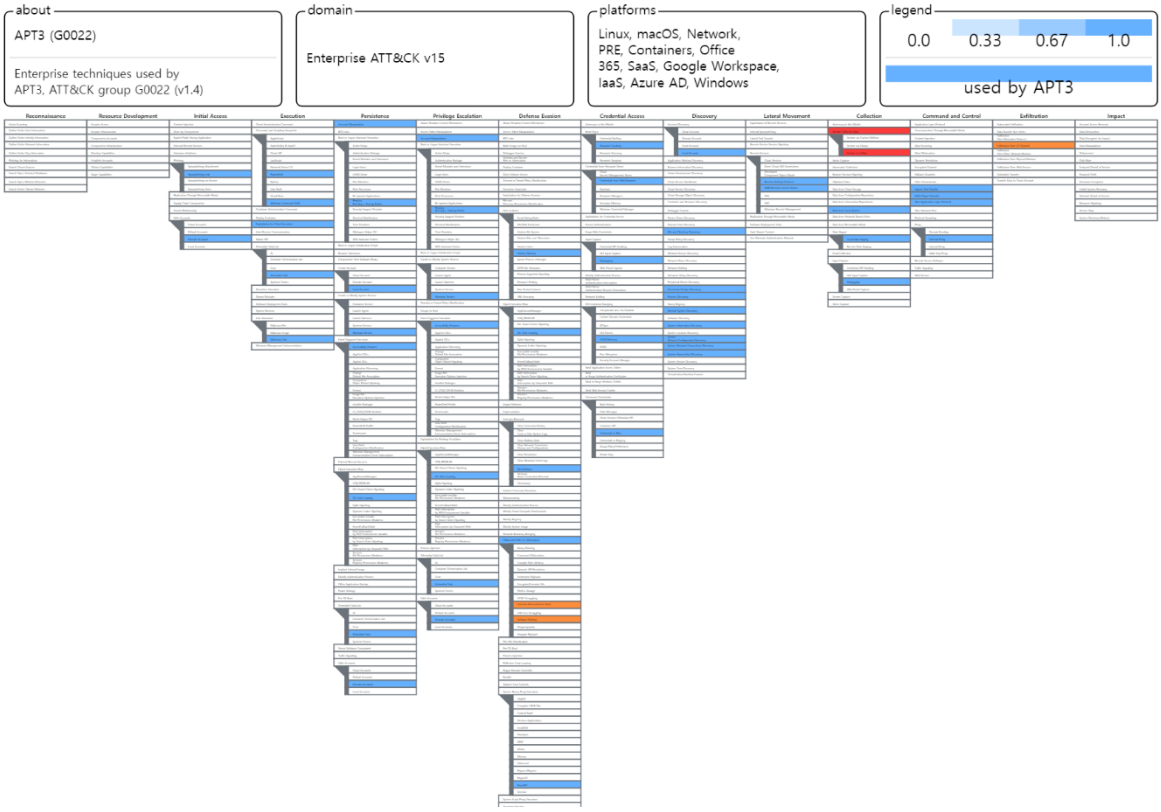

그림 4. APT3 group의 공격 시나리오를 Mitre Att&ck Navigator로 순서화 한 모습

- **공격 시나리오 작성**: 각 취약점을 이용한 공격 시나리오를 작성하여, 단계별 공격 절차를 상세히 기술한다.
- **위험 평가 및 우선순위 결정**: 각 시나리오의 위험도를 평가하고, 우선순위를 결정하여 테스트 및 구현 계획을 수립한다.

2.3 클라우드 환경 구축

설계된 공격 시나리오를 테스트할 수 있는 클라우드 환경을 구축한다. 이 단계에서는 다양한 클라우드 서비스와 인프라를 구성하여, 실제 환경과 유사한 테스트 베드를 마련한다. 주요 활동은 다음과 같다.

- **클라우드 인프라 설계**: 가상 머신, 컨테이너, 네트워크 구성 등을 포함한 클라우드 인프라를 설계한다.

- **환경 설정 및 배포**: 설계된 인프라를 Public Cloud(AWS, Azure, GCP 등) 혹은 Private Cloud(OpenStack)에 배포하고, 필요한 설정을 완료한다.

- **보안 설정 구성**: 테스트를 위한 보안 설정(방화벽, IAM 정책 등)을 구성하여, 다양한 보안 시나리오를 시험할 수 있도록 한다.

- **모니터링 및 로깅**: 공격 시나리오 실행 시 필요한 모니터링 및 로깅 기능을 설정하여, 결과를 분석할 수 있도록 준비한다.

2.4 자동화 도구 개발

구축된 클라우드 환경에서 설계된 공격 시나리오를 자동으로 수행할 수 있는 도구를 개발한다. 웹 프로그램, C/C++ 또는 Python 을 활용하여 작성하며, 공격의 자동화와 결과 분석 기능을 포함하는 플랫폼 형태를 목표로 한다. 주요 활동은 다음과 같다.

- **도구 설계 및 아키텍처 정의**: 공격 자동화 도구의 기능 요구사항을 정의하고, 시스템 아키텍처를 설계한다.

- **개발 환경 구축**: 개발에 필요한 소프트웨어 및 도구(IDE, 라이브러리 등)를 설치하고 설정한다.

- **공격 모듈 구현**: 각 공격 시나리오에 대응하는 모듈을 개발하여, 클라우드 환경에서 자동으로 공격을 수행할 수 있도록 한다.

- **결과 분석 및 보고 기능 구현**: 공격 수행 후 결과를 분석하고, 이를 시각화하여 보고할 수 있는 기능을 개발한다.

- **테스트 및 검증**: 개발된 도구를 다양한 시나리오에서 테스트하고, 성능과 정확성을 검증한다. 필요 시 피드백을 반영하여 개선 작업을 수행한다.

각 단계별로 체계적으로 진행하여, 최종적으로 클라우드 환경에서의 보안 위협을 효과적으로 탐지하고 대응할 수 있는 자동화 도구를 완성한다.

3. 연구 일정 및 역할 분담

3.1 연구 일정

#	항목	시작	종료	기간 (주)	날짜									
					6/3	6/17	7/1	7/15	7/29	8/12	8/26	9/9	9/23	10/7	10/18
1	기초 지식 공부 (Mitre Att&ck, CVE, Exploit, Cloud)	5/6	6/17	4											
2	클라우드 관련 보안 공격 분석	5/6	8/26	16											
3	공격 시나리오 설계	6/24	9/9	13											
4	클라우드 환경 구축	7/1	9/9	12											
5	자동화 도구 개발	8/26	9/23	4											
6	미흡한 점 보완 및 마무리	9/23	10/18	3.5											FINISH

3.2 역할 분담

학 번	이 름	역할
201824441	김승혁	IaaS 관련 보안 공격 분석 공격 시나리오 설계 클라우드 환경 구축 자동화 도구 개발
201824507	송재홍	SaaS 관련 보안 공격 분석 공격 시나리오 설계 클라우드 환경 구축 자동화 도구 개발
202145827	정재영	하이퍼바이저 대상 보안 공격 분석 공격 시나리오 설계 클라우드 환경 구축 자동화 도구 개발