


# 입 사 지 원 서

지원부문	정보보안	희망연봉	회사내규	
1. 인적사항				
성명	장진영 Jang Jin Yeong	생년월일	1997. 06. 19	
E-MAIL	<u>wkddud1793@gmail.com</u>	전화번호	010-6658-1793	
주소	대구광역시 북구 옥산로 17길 43-1 101호			

## 2. 학력 및 교육사항

기간		학교	학과(학점)	졸업구분
2016. 3 ~ 2025. 2		경북대학교	3.34/4.5	졸업
2013. 3 ~ 2016. 2		성광고등학교	-	졸업
교육사항	교육기간(총)	2024.09~2025.02 (872시간)	교육시간	09:00~17:50 (주5일)
	교육기관	코리아 IT 아카데미대구	교육과정명	정보보안
	교육내용			
	클라우드와 보안의 기본 개념과 특징 등 정보보안과 관련된 기반지식을 바탕으로 클라우드 보안 설계, 보안서비스 구축 실무 능력 함양과 클라우드 아키텍처 및 거버넌스를 수립할 수 있는 역량을 습득한 산업구조변화대응에 특화된 인재 양성			

## 3. 병역 및 기타사항

병역	필	군별	육군	계급	일병	기간	2017.04~2019.10	병과	보병
----	---	----	----	----	----	----	-----------------	----	----

## 4. 능력사항

구분	상세 보유기술
네트워크	라우팅, 스위치 구축 기술을 통하여 효율적인 네트워크망 구성 가능, Firewall 구성을 통하여 보안 설정 가능, IPT 서비스 구축 가능, 패킷 분석 가능
시스템	Window, Linux 서버 구축, WEB, DNS, FTP, MAIL, SAMBA, NFS 등의 서비스 구성, 방화벽 설정을 통해 보안 설정 가능
취약점분석/모의해킹	Window/Linux 취약점 분석(Nessus), 스캐닝을 통하여 취약점 분석, 스푸핑, 스니핑을 통하여 정보 획득 및 공격 metasploit 등의 툴을 이용한 모의해킹 가능, 스위치 및 라우터 보안 기능 설정 가능
악성 코드 분석	Flare를 활용한 악성코드 분석 환경 구축 가능, PEiD, IDA, OllyDbg 등 도구를 이용한 악성코드 정적/동적 분석 가능 악성코드의 동작 분석 및 트래픽, 시스템 영향 파악 가능

## 5. 기타 활동사항

기간	기관명	활동 내용 및 담당 업무
2021. 3~ 2021. 7	경북대학교 국제교류처	외국인 재학생의 전반적인 학교 생활 튜터링
2023. 7~ 2025. 2	메가MGC커피 대구 침산점	음료 제조, 재고 파악 및 손님 응대

## 6. 포트폴리오 주소

깃허브	<a href="https://github.com/jinyeong001">https://github.com/jinyeong001</a>
깃페이지	<a href="https://jinyeong001.github.io/jinyeong001/">https://jinyeong001.github.io/jinyeong001/</a>

# 자 기 소 개 서

1)지원동기	<p>‘산대특) DevSecOps를 활용한 클라우드 보안 전문가 양성 과정’을 통해 다양한 보안 관련 공부를 하고, 여러 모의해킹 관련 실습을 하며 모의해킹 결과보고서, 악성코드 분석보고서 등 다양한 보고서를 작성하는 경험을 가지게 되었습니다.</p> <p>또한 함께 공부한 동기들과 마지막으로 함께한 프로젝트에서 전체적인 가이드 문서 작성 업무를 하면서 보안 문서작성에 대한 흥미를 가지게 되었습니다.</p> <p>이러한 경험을 바탕으로 저는 보안 관련 문서작업을 할 수 있는 회사에 지원하게 되었습니다.</p>
2)성장과정	<p>대학시절 국제교류처에서 주관한 유학생과 1:1로 붙어 학교생활을 돕는 튜터링 시스템에 지원하며 한 학기동안 유학생의 학교생활을 도운 경험이 있습니다. 처음에는 혼자 여러 일을 해결하려는 성향이 강했지만, 유학생을 돕는 과정에서 도움을 주고받는 상호작용의 중요성을 깨닫게 되었습니다.</p> <p>이후, 튜터 학생이 큰 도움이 되었다고 국제교류처에 전하며 다시 한번 튜터 시스템의 기회를 준다는 전화를 받았을 때, 누군가를 돕는 일에서 오는 큰 보람을 느낄 수 있었습니다.</p> <p>이 경험을 통해 공동체 안에서 함께한다는 것의 가치를 실감하게 되었고, 팀플레이와 협력을 통해 더 큰 성과를 낼 수 있다는 점을 배울 수 있었습니다. 특히, 이후 다양한 팀 프로젝트를 수행하면서 팀원들과의 긴밀한 협력이 프로젝트의 성공에 얼마나 중요한지를 더욱 깊이 체감하게 되었습니다. 각자의 역할과 책임을 존중하며 목표를 향해 나아갈 때, 개인의 역량을 넘어서는 성과를 만들어낼 수 있다는 것을 배웠습니다.</p> <p>이러한 경험을 통해 성장한 제 가치관은 앞으로 회사에 입사하여 팀원으로서의 역할을 충실히 수행하는 데에도 큰 밑거름이 될 것입니다. 팀의 목표를 위해 협력하고, 동료들과 함께 시너지를 만들어내는 모습으로 회사의 발전에 기여하고 싶습니다.</p>
3) 성격의 장단점	
4) 입사 후 포부	<p>저는 보안 전문가로서 성장하고 싶은 사람입니다. 전문가의 기준은 다양할 수 있지만, 하나의 지표로서 보안 관련 자격증은 제 성장의 방향성을 확인할 수 있는 중요한 기준이라고 생각합니다. 그래서 저는 현재도 자격증 공부를 꾸준히 진행하고 있으며, 매년 목표로 삼은 자격증을 통해 저의 성장을 확인하고 있습니다.</p> <p>입사 후에도 이러한 목표를 지속해서 설정하며 보안 및 네트워크 관련 자격증 취득을 위해 꾸준히 노력할 것입니다. 이를 통해 전문성을 갖춘 보안 전문가로서 성장해 나갈 것입니다.</p>
5)직무관련 경험	<p>몇 개의 팀 프로젝트를 진행하면서, 대부분의 문서작업 임무를 도맡아 하게 되었습니다. 프로젝트의 목표와 진행 과정을 설명하는 글을 작성하면서, 제가 참여한 일의 의미와 가치를 되새길 수 있었고, 이를 통해 큰 보람을 느꼈습니다.</p> <p>단순 문서 작성뿐만 아니라, 소속 팀의 Gitpage, Git 프로필에 보이는 README파일 작성, IDS 룰 작성, 그리고 개인적으로 수행한 다양한 보고서 작성 경험을 통해 제 보안지식과 업무 이해도를 점검하고 더욱 심화할 수 있었습니다. 특히, DevSecOps 보안 가이드 문서 작성 프로젝트에서는 기획팀장을 맡아 팀원들을 관리하고, 각 팀원의 능력과 업무 진행 상황을 파악하며 프로젝트 일정을 조정하는 등의 경험을 쌓았습니다. 이러한 경험은 팀 전체의 효율성을 높이고 목표를 효과적으로 달성할 수 있는 방법을 배우는 계기가 되었습니다.</p> <p>이 과정에서 저는 팀원들과의 원활한 소통과 협력의 중요성을 실감하였고, 이를 통해 공동 목표를 달성하는 데 있어 팀원과의 소통과 정보 공유가 중요한 역할을 한다는 점을 깊이 깨달았습니다.</p> <p>앞으로 저는 이러한 경험을 바탕으로 팀원들과의 소통과 팀플레이를 바탕으로 보안 문서 작성과 체계적인 업무를 수행하며, 회사와 팀의 발전에 기여하는 사람으로 성장해 나갈 것입니다.</p>

# 프로젝트 소개서

수행 프로젝트	항목	주요내용
	프로젝트 명	2025 DevSecOps 환경 구축 가이드
	수행기간	2024.12. ~ 2025.02 (3개월)
	목표	<p>2025 DevSecOps 환경 구축 가이드는 DevSecOps 방식을 통해 개발, 운영, 보안을 효과적으로 통합하여 CI/CD 프로세스를 최적화하고 시스템의 안전성을 강화하는 방법을 제시합니다.</p> <p>특히, Jenkins, SonarQube, Docker, Kubernetes와 Wazuh을 활용하여 소스코드 품질을 개선하고 보안 자동화를 구현하는 구체적인 접근법을 제공합니다.</p>
	내용	<p>Kubernetes를 활용하여 하나의 통합된 환경을 구축하고, Jenkins, Github를 통하여 소스코드의 변화가 생겼을 때, 빌드 및 재배포를 자동화하여 효율적인 빌드 및 배포 프로세스를 구현하였습니다.</p> <p>Kubernetes 기반으로 확장이 자유롭게 가능하고, 안정적인 애플리케이션 실행 환경을 설계하였습니다.</p> <p>또한 모니터링을 위하여 Wazuh를 활용하여 시스템 로그와 보안 이벤트를 통합 관리하여, 빠른 문제 분석과 대응이 가능합니다.</p> <p>DevSecOps를 통해 개발, 운영, 그리고 보안 팀 간의 긴밀한 협력을 통하여 조직 전반의 보안 인식을 제고할 수 있습니다.</p> <p>본 가이드의 핵심은 DevSecOps의 환경을 누구나 구축하고 운영할 수 있기 위함으로, '2025 DevSecOps 환경 구축 가이드'는 이러한 모든 과정을 세세하게 적고 설명한 DevSecOps 기초 가이드입니다.</p>
	설계/프로세스	DevSecOps 환경 구축을 위한 가이드 문서 제작 및 배포
	담당 역할	<ol style="list-style-type: none"><li>'2025 DevSecOps 환경 구축 가이드' 문서의 전반적인 작성 및 수정</li><li>문서를 기반으로 GitPage 구축</li><li>Jenkins와 Github를 이용한 CI/CD 파이프라인 구축 및 자동화</li><li>프로젝트 진행 상황 파악과 팀원들에게 담당 역할 분배 및 조정</li></ol>
	느낀점/성장점	<p>이 프로젝트는 실제 필드의 경험을 위하여 개발팀, 운영팀, 기획팀 총 3개의 팀으로 나누어 진행되었습니다. 저는 기획팀으로서 일을 하게 되어 초기에 전체적인 프로젝트 기획을 통해 방향성을 정하는 것에 많은 시간이 투자된다는 것을 느꼈습니다.</p> <p>또한 가장 크게 느낀 점으로는 나의 팀만 아니라 함께 협업하는 다른 팀의 진행 상황을 항상 함께 체크해야 한다는 것입니다. 실제 테스트를 진행하며 가이드 문서를 작성하는 임무를 수행하기 위하여 지속해서 개발팀과 소통을 해야 했고, 이 과정을 통하여 팀 간의 소통의 중요성을 느꼈습니다.</p> <p>서로 소통이 활발하였기 때문에, 막히는 부분이 있었을 때 빠르게 대응할 수 있었습니다. 이 모든 과정을 통하여 개인이 아닌 팀이 얼마나 중요한지 알게 되었고, 소통이 팀 프로젝트에 기여하는 바가 큰 것을 느꼈습니다.</p>

수 행 프 로 젝 트	항목	주요내용
	프로젝트 명	CTF Ignite
	수행기간	2024.09. ~ 2025.10 (1개월)
	목표	CTF 머신 제작을 통해 여러 상황에 대한 취약점을 분석하고 대응할 수 있는지에 대한 경험을 제공합니다. 특히, Web, Database, Linux와 Docker의 환경에서 Injection, 권한 탈취 등의 취약점을 점검할 수 있는지에 대한 정보를 제공합니다.
	내용	여러 CTF를 통해 터득한 모의해킹의 경험을 토대로, 스스로 CTF 머신을 제작하여 더욱 여러 상황에서의 취약점을 점검할 수 있는 경험을 위하여 'CTF Ignite' 프로젝트를 시작하였습니다.
	설계/프로세스	
	담당 역할	
	느낀점/성장점	

항목	주요내용
프로젝트 명	Flame War Game
수행기간	2024.10. ~ 2024.12 (2개월)
목표	Flame War Game을 통하여 웹 보안 학습을 위한 실전 위게임 플랫폼 구축하여 40개 이상의 단계별 문제를 통해 다양한 웹 취약점을 학습하고 실습할 수 있는 환경을 제공합니다.
내용	<p>Flame은 다양한 웹 보안 문제뿐만 아니라, Linux, DB, Script 조작 등 다양한 취약점 문제를 제공하여 실습할 수 있는 환경을 제공합니다.</p> <p>Flame의 특징으로는 사용자 시스템과 관리자 시스템이 있습니다. 회원가입 및 로그인 기능을 구현하여 계정을 관리하고, 가입된 계정의 닉네임을 이용하여 Database를 구축하여 개인별 학습 진도 추적이 가능합니다.</p> <p>또한, 관리자 페이지를 구축하여 시스템 모니터링 및 여러 관리 도구를 이용할 수 있습니다.</p> <p>이렇게 구축한 모든 환경은 Docker Image로 만들어 배포하여 사용자에게 Linux 기반 컨테이너 환경을 제공하고, 자동화된 설치와 사전 구성된 환경을 즉시 서비스 실행할 수 있게 합니다.</p>
설계/프로세스	HTML5, CSS3, JavaScript, PHP, Apache, MariaDB, .htaccess
담당 역할	<ol style="list-style-type: none"><li>1. Web 구축 및 CSS를 통한 전반적인 웹 스타일 제작</li><li>2. Database 구축 및 Schema 설계</li><li>3. 회원가입 및 로그인 시스템 구축</li><li>4. 랭킹 시스템, 관리자 페이지 구축</li><li>5. 팀원들과 함께 다양한 웹 보안 문제 제작</li></ol>
느낀점/성장점	<p>여러 보안 취약점들을 활용하여 문제를 만들면서 다양한 취약점에 대하여 스스로도 학습할 수 있게 된 프로젝트였습니다.</p> <p>문제를 모두 만든 후, 서로 테스트하면서 다양한 버그를 발견하면서 아무리 열심히 만들었더라도 버그가 생길 수 있다는 것과 테스트의 중요성을 다시 한번 실감했습니다.</p> <p>Database 설계를 하면서, 얼마나 실용적으로 Schema를 제작하는 것이 어려운지와 초기 Schema 설정에 따라 데이터 저장의 난이도가 달라지는지를 경험할 수 있었습니다.</p> <p>또한, 내가 생각하지 못한 취약점에 대한 문제를 다른 팀원이 찾고, 만들었을 때를 생각하면 팀으로서 함께 프로젝트를 하는 것에 대한 중요성과 팀워크를 경험할 수 있어 좋았습니다.</p>

수행 프로젝트	항목	주요내용
	프로젝트 명	Linux 취약점 분석 Shell Script
	수행기간	2024.09. ~ 2024.09 (2주)
	목표	Rocky Linux 환경의 기술적 취약점을 분석하고 취약한 부분을 알려주는 Shell Script 작성을 통하여 Shell Script 작성법과 다양한 Linux의 취약점 관리 기술 터득
	내용	<p>2021년 과학기술정보통신부와 한국인터넷진흥원이 배포한 ‘주요 정보통신기반시설 기술적 취약점 분석·평가 방법 상세 가이드’에 적힌 유닉스 서버의 취약점 점검 항목을 토대로 Rocky Linux의 취약점 점검 Shell Script를 작성하였다.</p> <p>해당 스크립트를 실행하면 계정관리, 파일 및 디렉터리 관리, 서비스 관리, 패치 및 로그 관리로 총 72가지의 항목을 점검하는 스크립트가 실행된다.</p> <p>스크립트가 실행되면, 가이드에 적혀있는 판단기준을 토대로 각 점검 항목마다 양호 또는 취약이라는 문구가 출력되며 해당 점검 항목이 나타난다.</p> <p>Shell Script에 기능을 추가하여, 모든 점검 항목 출력, 취약한 점검 항목만 출력, 단순 출력 및 출력 파일을 텍스트화하여 저장할 수 있는 기능을 추가하였다.</p>
	설계/프로세스	
	담당 역할	1. Rocky Linux에 없는 점검 항목 파악 및 작성할 점검 항목 분류 2. 계정 관리 및 서비스 관리 점검 항목 스크립트 작성
	느낀점/성장점	Shell Script를 작성하는 방법을 알게 되었고, Unix 기반 환경에서 조심해야 할 다양한 취약점들에 대한 지식을 얻는 계기가 되었다. 또한 한국인터넷진흥원에서 배포하고 있는 다양한 보안 가이드 문서에 대하여 알게 되어 보안 공부에 있어 큰 도움이 되었다.