# 네트워크 보안 실무 프로젝트 준비 및 자기소개서 활용 전략

## 1. 실전 프로젝트용 핵심 기술 영역

|  |  |  |  |
| --- | --- | --- | --- |
| 영역 | 기술 내용 | 프로젝트 예시 | 이력서/자소서 활용 포인트 |
| 네트워크 보안 기초 | OSI 7계층, TCP/IP, 패킷 구조, 포트 개념 | Wireshark로 TLS 분석, Socket 통신 프로그램 | 네트워크 구조에 대한 이해를 바탕으로 시스템을 설계 |
| 암호화/인증 기술 | 대칭키/비대칭키, RSA, AES, 해시, SSL/TLS, JWT | TLS handshake 구현, JWT 기반 로그인 서버 | 공개키 기반 구조(PKI) 적용 경험 |
| 공격·방어 실습 | ARP Spoofing, MITM, DNS Spoofing, Sniffing | 공격 시뮬레이터 구축, 탐지 시스템 개발 | 보안 위협 탐지 및 대응 설계 경험 |
| Socket 프로그래밍 | TCP/UDP 클라이언트-서버 통신 구현 | 채팅 서버, VPN/프록시 구조 실험 | 실제 통신 흐름을 설계 및 구현한 경험 |
| 패킷 분석 도구 활용 | Wireshark, tcpdump, scapy, pyshark | 실시간 패킷 로깅, 이상 트래픽 탐지 | 네트워크 흐름 분석 및 시각화 경험 |
| 시스템 보안 도구 | iptables, netstat, nmap, ufw, OpenSSL, Docker | 방화벽 설정, 인증서 발급 및 적용 | 운영체제 보안 설정 및 인증서 적용 경험 |
| 웹 인증/보안 프로토콜 | HTTPS, OAuth2.0, JWT, CORS | 로그인/세션 시스템 구축 | 웹 보안 구조에 대한 이해 및 구현 경험 |

## 2. 공부 과정 (8주 완성 플랜 예시)

● 1~2주차  
네트워크/보안 이론 + 기본 실습  
- OSI 7계층, TCP/IP, 포트 개념 정리  
- Wireshark로 HTTP, HTTPS 요청 캡처  
- netcat, ping, traceroute 실습  
- 패킷 구조 및 통신 흐름 요약

● 3~4주차  
Socket 통신 구현 + TLS/암호화 기초  
- Python TCP 클라이언트-서버 제작  
- OpenSSL로 인증서 발급 및 적용  
- RSA, AES, SHA256 실습  
- JWT 로그인 API 구성

● 5~6주차  
보안 공격 실습 + 탐지 시스템 구현  
- ARP Spoofing, DNS Spoofing, MITM 시뮬레이션  
- Snort 또는 Scapy로 IDS 설계  
- 패킷 필터링 및 로깅 시스템 구축

● 7~8주차  
종합 프로젝트 구현 + 발표/정리  
- 보안강화 통신 채널 + IDS 기반 모니터링  
- Docker 구성, REST API 통합  
- 시스템 구성도 및 발표 자료 정리

## 3. 자기소개서 문장 예시

“종합설계 프로젝트에서는 네트워크 보안 통신 구조를 주제로, TLS 기반 클라이언트-서버 구조를 직접 구현하고, MITM 공격 시나리오를 가상 환경에서 시뮬레이션했습니다. 이 과정에서 JWT 기반 인증 토큰 설계, OpenSSL 인증서 발급 및 적용, IDS 탐지 시스템을 직접 구성하며 보안 통신에 대한 실무적 이해를 쌓을 수 있었습니다. 문제를 단순히 이론적으로 접근하는 것이 아니라, 실제 통신 흐름을 추적하고 구조화하는 데에 집중하며 실전 역량을 키웠습니다.”

## 4. 추천 학습 리소스

● 네트워크 이론: 생활코딩 - 인터넷, 고려대 김기현 교수 TCP/IP 강의

● 보안 실습: picoCTF, Hack The Box

● Wireshark 실습: Wireshark 공식 튜토리얼

● Socket 프로그래밍: Python socket 공식 문서, Go net 패키지

● JWT 인증 실습: Auth0 JWT playground

● 오픈소스 IDS: Snort, Suricata GitHub