**# 2022 겨울방학 프로젝트 아이디어 1**

- IoT 네트워크 취약점을 이용한 ARP 스푸핑 공격 실습

- 중간자 공격을 통한 패킷 위변조 or 접근 제어 우회(권한 상승)

\*ARP Spoofing Attack : MAC 주소를 IP로 변환하는 프로토콜로서 통신하는 두 대상의 MAC 주소를 공격자 자신의 MAC 주소로 바꾸어 중간에서 패킷을 가로채는 공격

\*중간자 공격(Man in the Middle) : MITM 중간자 공격은 ARP 스푸핑에 의존하여 피해자 간의 트래픽을 가로채고 수정

**# 프로젝트 설명**

아두이노를 통해 IoT기기를 제작, 추후 사용자와 IoT 기기 사이에 프록시 역할을 하는 공격자가 ARP spoofing 공격을 통해 희생자와 IoT기기간의 통신을 도청 -> 수집한 패킷을 통해 민감 정보를 탈취하고, 패킷을 위·변조해 IoT 기기를 익스플로잇 (+수집된 패킷을 통한 권한 상승 공격, +UDP Flooding을 통한 DDOS 공격)

\*제작할 IoT 기기는 되도록 민감한 데이터를 다루는 IoT기기로 선정(팀원들과 상의)

**# 프로젝트 진행 순서**

1. 아두이노를 이용한 IOT 기기 제작
2. IOT 기기 취약점 분석
3. ARP spoofing을 통한 패킷 수집
4. 패킷 분석을 통한 크리덴셜 탈취
   1. 수집한 패킷을 변조하여 IOT 기기 익스플로잇
   2. 수집한 패킷를 통한 권한 상승
5. 보고서 작성

**#참고자료**

<https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project>

<https://southern-island.tistory.com/22>

<https://ddongwon.tistory.com/48>

<https://kkomii22.tistory.com/54>

**# 2022 겨울방학 프로젝트 아이디어 2**

- IOT에 악성코드를 주입하여 봇넷 생성 -> DDoS 공격에 활용 (미라이봇넷 모방 실습)

\*봇넷 : 악성 소프트웨어에 감염되어 악성 행위를 하도록 원격으로 조종 되는 다수의 좀비 컴퓨터들의 네트워크

**# 프로젝트 설명**

아두이노를 통한 IoT기기를 제작, 추후 IoT기기를 스캐닝해 열려 있는 포트를 찾아내 악성코드에 감염시킴. 추후 해당 IoT를 통해 DDoS 공격에 활용 (미라이봇넷 모방 실습)

\*미라이봇넷 동작원리: 관리자 계정설정이 취약한 임베디드 기기(CCTV, NAS 등) 스캐닝˙접속→ 악성코드 전파 및 감염 → 취약한 기기 감염으로 좀비 PC 확보 → 봇넷 구성 → 봇넷을 이용한 디도스 공격

**# 프로젝트 진행 순서**

1. 아두이노를 이용한 IOT 기기 제작
2. 악성코드 제작
3. IOT 기기 포트 스캐닝
4. 오픈 되어 있는 포트를 통해 악성코드 감염
   1. 감염된 IoT기기로 봇넷 구성
   2. 구성된 봇넷으로 DDoS 공격
5. 보고서 작성

**#참고자료**

<https://www.techtarget.com/iotagenda/tip/5-IoT-security-threats-to-prioritize>

<http://wiki.hash.kr/index.php/%EB%AF%B8%EB%9D%BC%EC%9D%B4_%EB%B4%87%EB%84%B7>

<https://metamong3.tistory.com/7>