3주차 – 칼리리눅스

<http://165.194.29.112/> 여기다 공유박스 많이 씀

터미널 – 명령어 창

명령어 wget <http://165.194.29.112/modbusPal.jar> 입력

파일이 리눅스 환경에서 다운 받아짐.

칼리 리눅스는 기본적으로 자바가 설치되어있음.

Java –jar ModbusPal.jar 입력 -> Modbuspal 1.6b 실행 (1)

외부에서 열려있는 포트를 찾아보자 - 터미널 – 뉴 윈도우

포트 : 서비스와 연결되는 게이트

http(웹서비스) – 80/TCP https(암호화웹) – 443/tcp

nmap 도구 – 서버의 포트 오픈 여부 확인

nmap 192.168.124.128 –p 모든 포트를 확인 (2)

service apache2 start

root@kali:~# service ssh start (2) 임의적으로 서비스를 연다.

nmap 192.168.124.128 -p-

<https://www.shodan.io/explore/category/industrial-control-systems> 쇼단에서 우리가 실제로 보는 애.

모드버스를 클릭 – 포트 502라고 찾는다.

Unit ID: 0

-- Slave ID Data: Illegal Function (Error)

-- Device Identification: Illegal Function (Error)

Unit ID: 0

-- Slave ID Data: Illegal Function (Error)

-- Device Identification: Illegal Function (Error)

Unit ID: 1

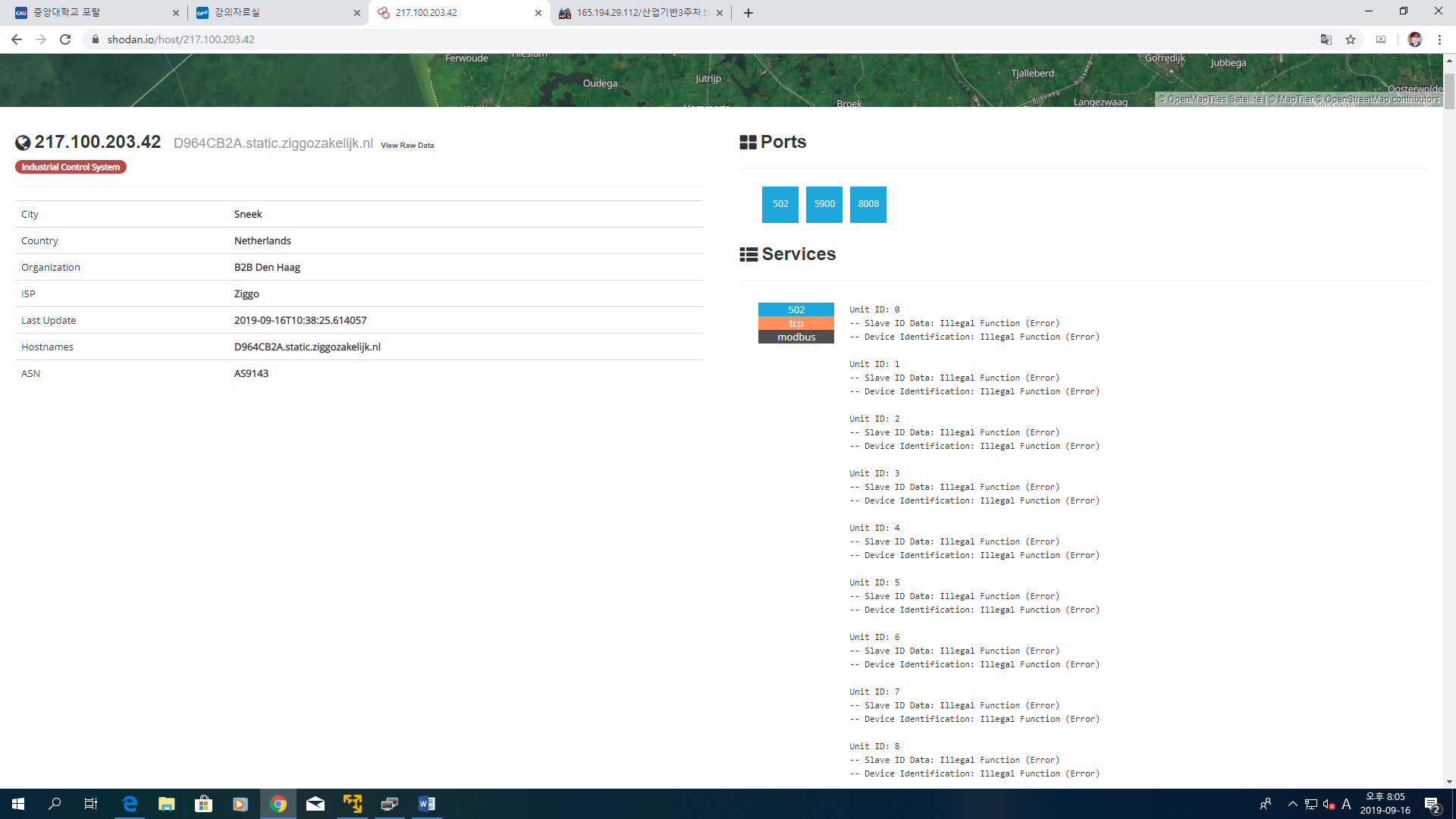
-- Slave ID Data: Illegal Function (Error)

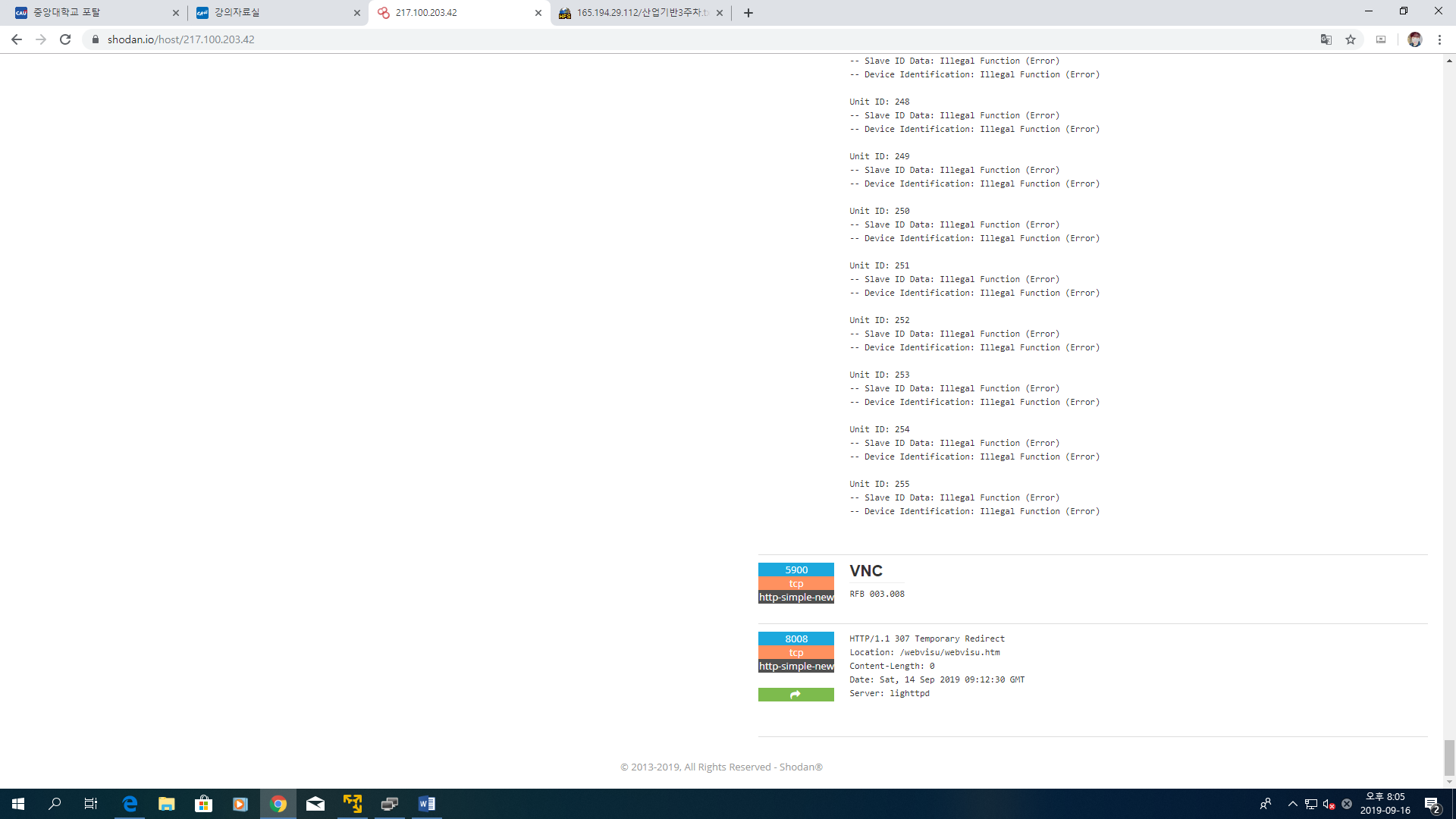
-- Device Identification: Illegal Function (Error)

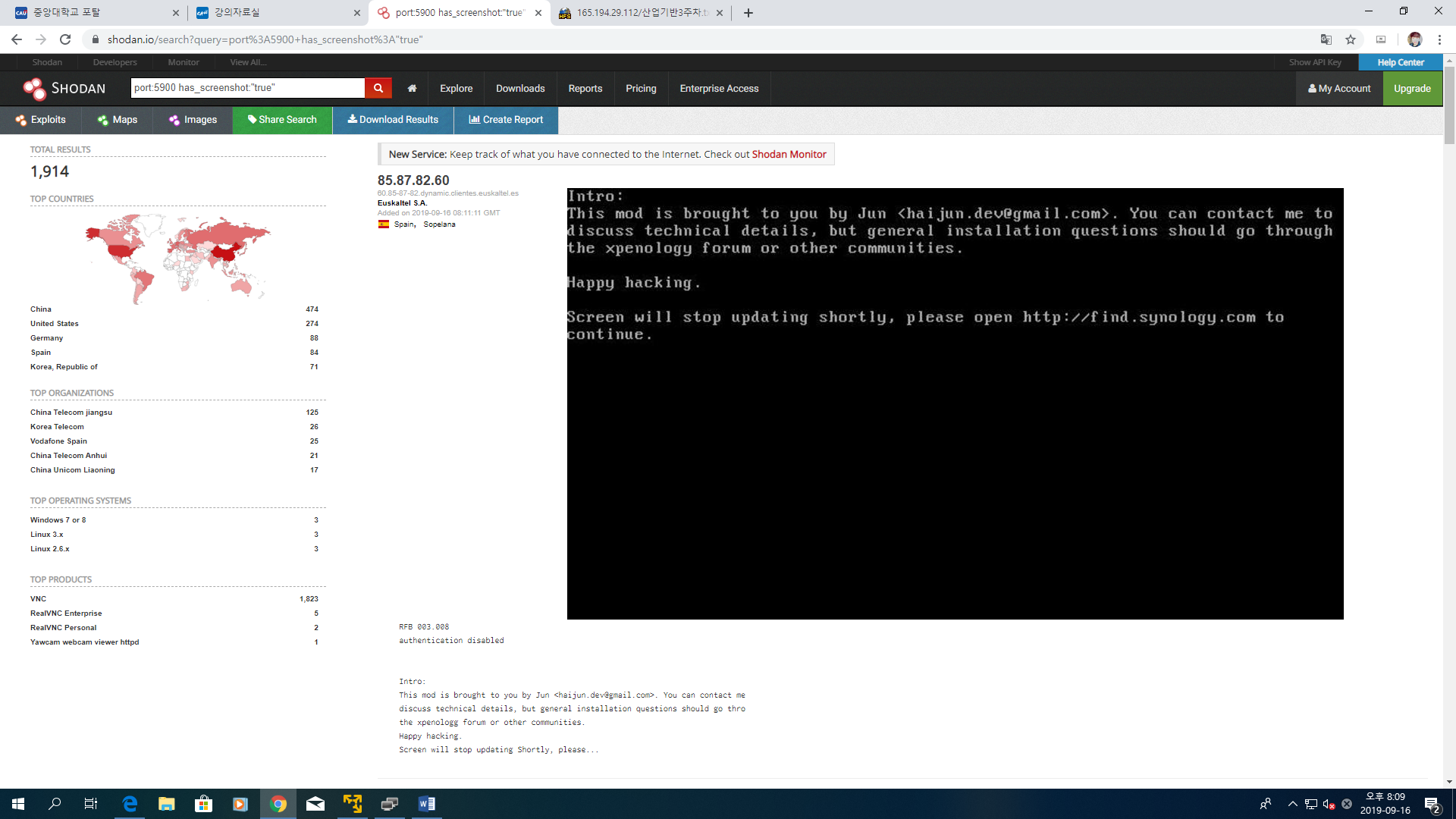
Unit ID: 2

-- Slave ID Data: Illegal Function (Error)

-- Device Identification: Illeg...

---🡪 Modbus 서버에서 만든 것 // modbuspal에서 add – slave 만든것 – 이것이 노출된 것이다.ㅍ

모드버스 관련 슬레브의 정보가나옴. VNC는 원격터미널서비스 중에 하나. (원격 데스크텁 연결과 거의 동일한 역할) / 장비를 제어할 때.

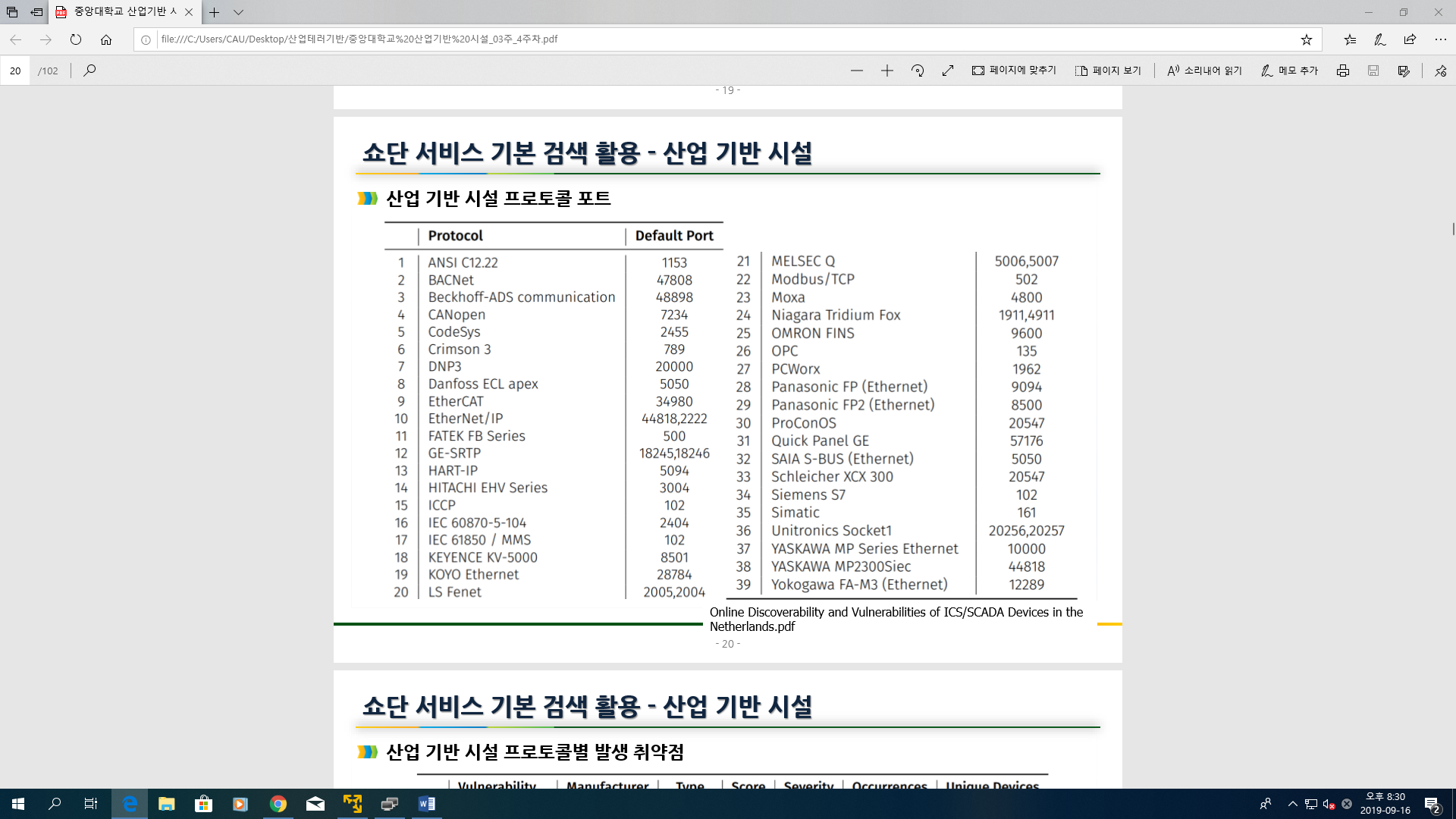


제어장치들의 화면. 포트5900은 VNC가 사용하고 있는 포트 / 원격 서비스이다.’VNC는 /

OSINT :누구나 정보에 접근해서 정보를 얻을 수 있는 서비스. 트이터, 페북, 구글,

VNC = 원격 서비스 (화면으로제어\_ - 5900 / TCP

* 산업기반 시설에서 화면을 제어하기위한 목적 -> PLC -> 장비 제어



Pdf 20페이지 중요. 외울필요 X // Modbus 502 / Siemens S7 102 / DNP3 20000 /

**Common Vulnerabilities and Exposures : 공통 취약점 및 발생하는 / 취약점들에 넘버값을 적음, 각 넘버값은 유일한 값이다.**

**P22 참고만하세요.**

**P15 쇼단 서비스 기본 검색 옵션 – 그 도메인을 가지고 있는 것을 검색해라.**

**서브 도메인 EX) Blog.aver.com / café.naver.com /**

**쇼단 : hostname:naver.com // Google.com 입력**

**net:165.194.1.0/24 - 중앙대학교 // 탑서비스에 http , https는 정상 / 264는??**

**country:"KR" has\_screenshot:"true" // --< 저번처럼 이런식으로 시험 나옴.**

**몽고DB : 포트 27017**

**몽고디비 중에서 인증이 되지 않은 서버 검색 명령어 ~~~**

**P28 쇼단 명령어 참고**

**P25 ~ p 3~~~~까지 쇼단 활용 내용**