산업기반테러시설 10.7

산업 시스템 제어 // 시스템 구조는 익혀야함.

중간고사는 서술 + 실습 / 1주차 강의자료를 외우지말고 이해를 하세요.

외운대로 쓰지마라. 어느정도만 맞아도 됨.

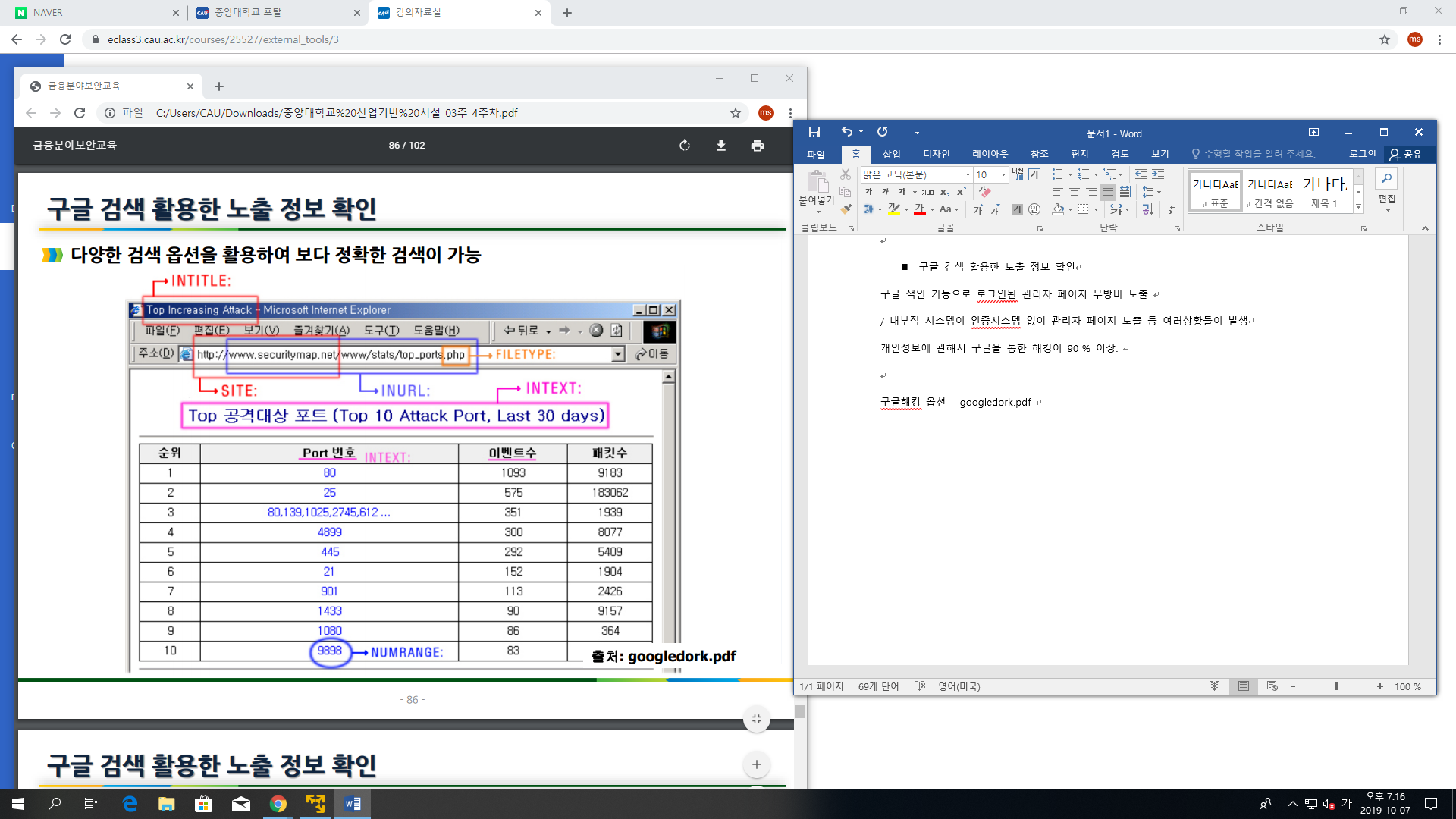
* 구글 검색 활용한 노출 정보 확인

구글 색인 기능으로 로그인된 관리자 페이지 무방비 노출

/ 내부적 시스템이 인증시스템 없이 관리자 페이지 노출 등 여러상황들이 발생

개인정보에 관해서 구글을 통한 해킹이 90 % 이상.

구글해킹 옵션 – googledork.pdf // 외우셈



Site:naver.com // 네이버.com 도메인을 가진 애들만 검색이 됨.

Stie:naver.com –site:www.naver.com // 도메인에서 [www.naver.com](http://www.naver.com) 검색어를 제외시켜라. (서브도메인만 확인하겠다.)

Site:naver.com inurl:admin // naver.com 에서 url정보에 admin이라는 검색어를 찾겠다. 검색이 될수도 있고 안될수도 있다. (일반적으로 관리자페이지)

Filetype:pdf,doc,xls

Ext:zip,log,tar 파일타입은 filetype , ext로 나눠지는데, 약간 검색파일의 종류가 다르다.

Site:naver.com inurl:admin filetype:xls -- > 네이버 도메인에서 admin의 url이 있는 주소에서 xls 확장자명을 가진 파일이 구글에 검색이 되는지 / 옵션 활용 방식

Intext : 웹페이지에 노출되는 문자열들을 확인하는 옵션 //페이지안에 어떤 정보들이 있다.

Site:naver.com inurl:admin intext:password

* Google 해킹 사례

사이트의 디렉터리 목록이 노출된 것을 검색

<title>태그는 모든 웹페이지에 하나가 있다. ( 페이지소스에서 )

<title>NAVER</title> --< 이것이 intitle이다.

intitle:index of // index of는 디렉터리 구조가 노출된 것.

Site:cau.ac.kr intitle:index of

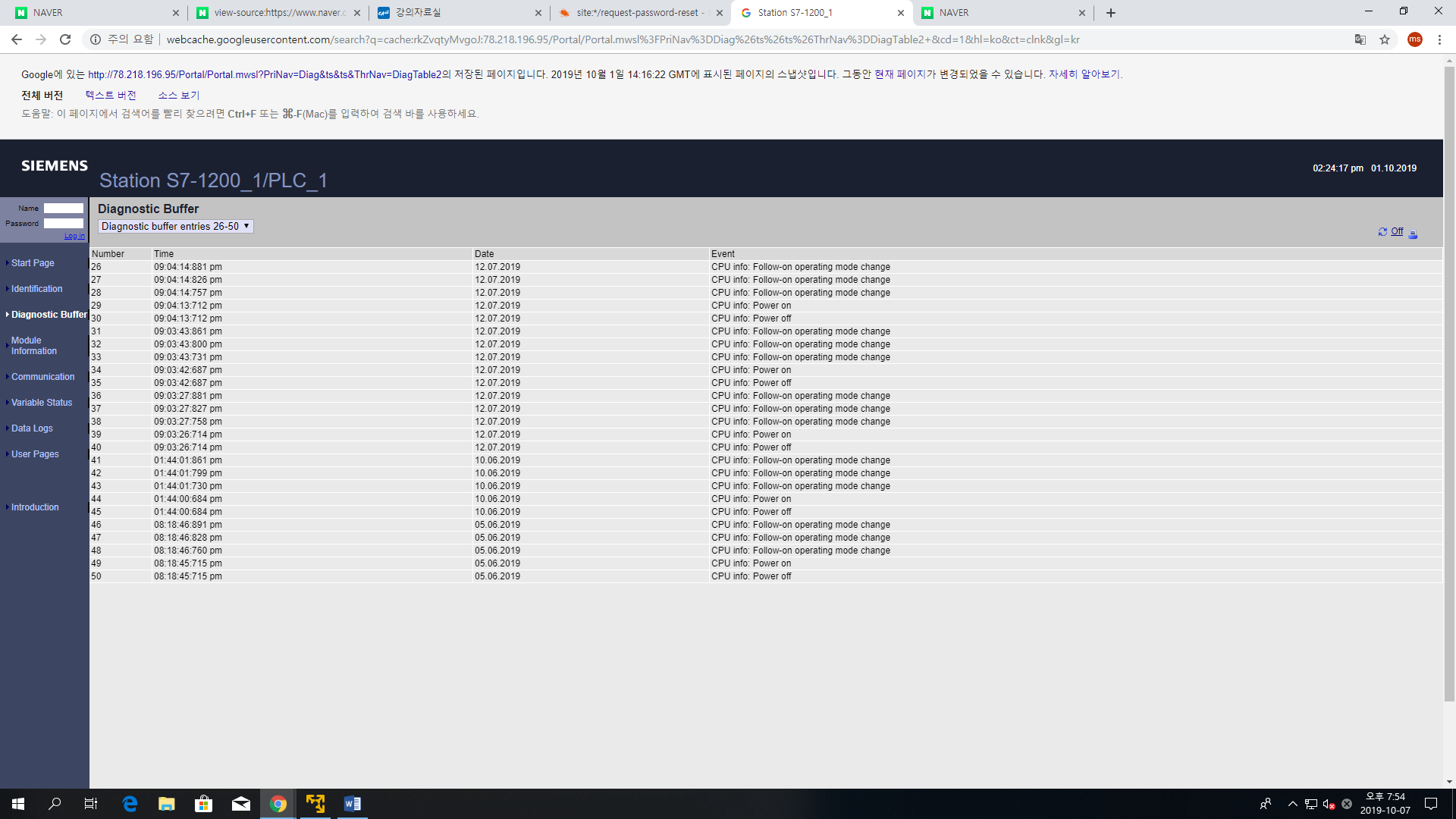
<https://www.exploit-db.com/> -- 공격코드가 포함된 사이트.

우리가 볼건 GHDB

Site\*~~~~wp //wp는 워드프레스 (컨텐츠 관련 서비스)

* 스카다 시스템 대상으로 구글 해킹 사례

inurl:/portal/portal.mwsl – 모두 취약하다고는 할수없으나, 외부에 노출되는 것들은 공격가능성이 존재함.

이런 정보들이 노출되면 안됨. // 모니터링 등 내부정보가 외부에 노출된 화면.

Scadasecuritybootcamp.com/scada-google-dorks.php (scada 시스템의 많은 정보를 담고있음)

여기서 SCADA Default Passwords는 스카다 시스템에 대한 유저 패스워드 정보 획득.

* Modbus – 설치, 통신여부? – Port 502를 사용함.

외부서비스 노출 여부 / 패킷정보 확인.. 조작여부 확인.

모드버스를 이용한 접속

칼리에 gem install modbus-cli

Ifconfig - modbus read 192.168.84.128 1 2 (1 2는

Modbus wirte 192.~~~ 2 1 / 3 0 / 4 1 등등으로 사용

Scada시스템에 기본적으로 사용하는 포트들이 외부에서 접속이 되면 100%공격이 가능함.

* Wireshark

Capture 기능 – 통신되는 정보를 확인.

와이어샤크 실행된 상태에서 Modbus read 와 write를 사용하고 패킷을 보는 과정.

리눅스상에서

modbus read 192.168.84.128 1 8

Modbus wirte 192.168.84.128 1 3 입력.

와이어샤크에 modbus의 패킷이 나옴.

Modbus를 필터링

와이어샤크 상에서 .000 0001= Modbus Function code : Read coils (1) 클릭하면

자릿수가 나온다.

* Funtion code는 무엇인가?

장표는 시험에 안냄. // FC=01은 코일상태 읽기 ,

와이어샤크 read를분석하면

Query: trans: -- 클라이언트 -> 서버

Response: trans: 서버 -> 클라이언트

와이어샤크 write unit: 1, func: 15 wirte multiple coils이라고 나옴.

* Statistics 옵션

Protocol hierarchy : 어떤 패킷들이 들어가있는지 종합적으로 확인가능한 옵션

* 모드버스 정리
* 공격자(범죄자) 입장에서

1. IP정보를 알아야함.
2. ip에서 어떤 포트가 오픈되어 있는지 확인

* Nmap 도구 활용
* Shodan 서비스 등 활용

1. Port:502가 오픈되면 – 서비스 접속이 가능하다 판단.
2. Read, write가 가능한지 확인

🡪 패킷분석을 해본거죠.