10.10 산기테

교재 16p 8주차

Git clone <https://github.com/riptideio/pymodbus.git>

Cd pymodbus

Pip install –r requiremetns.txt

pip install prompt\_toolkit –upgrade

**python setup.py install**

* pymodbus.console 활용 // 지원되는 프로토콜 도움말 확인

pymodbus.console tcp --help

pymodbus.console tcp --host 192.168.84.128 --port 502 // 모드버스 서버에 접속

client.read\_device\_information unit=1

시리얼 : 기기에 직접적으로 통신하는 경우,

client.read\_device\_information unit=1 // 슬레이브 하나에 대한 정보 읽어라.

개발 환경을 만든 것임.

Client.read\_holding\_registers address=0 count=10 unit=1 // 1슬레이브의 레지스터를 10번까지 읽어라. 🡪 레지스트리 값에 등록되어 있는 값을 원격에서 확인 가능

--------------------wire shark --------------------------

와이어 샤크에서 Modbus 필터링해서 / 읽은거 확인 및 분석 할 수 있음.

Client.write\_registers values=10,11,12 unit=1 address=0

레지스트리 공간에 원격으로 값을 수정

⚫ client.write\_registers values=10,11,12 unit=1 address=0 / 0번째부터 시작해서 (modbus프로그램에서는 1번째임) 1번째 2번째 3번째의 값을 10,11,12로 변경

* CIA 와 ACI는 시험에 나옴 (IT, OT)

산업제어 시스템에서 사용하는 프로토콜이 유출 -> 기밀성이 훼손됨.

Coil을 write할수 있음 -> 무결성 훼손

산업제어 시스템에서 현재까지 한 것을 이용해서 SCADA시스템과 연결된 IP를 다 연결해서 코일 레지스터 값들 바꾸면 해킹되는 원리

* Cpppo 파이썬 모듈데이터 정보 조작 // 이건 안했음.

PLC 데이터 조작과 비슷한 원리로 이더넷/IP cpppo 원격 접속 모듈에서도 데이터 정보 조작이 可

Python –m cpppo.server.enip SCADA=INT[1000] –v

* 공격 프레임워크를 이용한 취약점 진단 // p.34부터

Git clone <https://github.com/Exploit-install/smod>

Ls

Python smod.py

Help

Show modules

use modbus/scanner/uid

show options

set RHOSTS 192.168.84.128

exploit

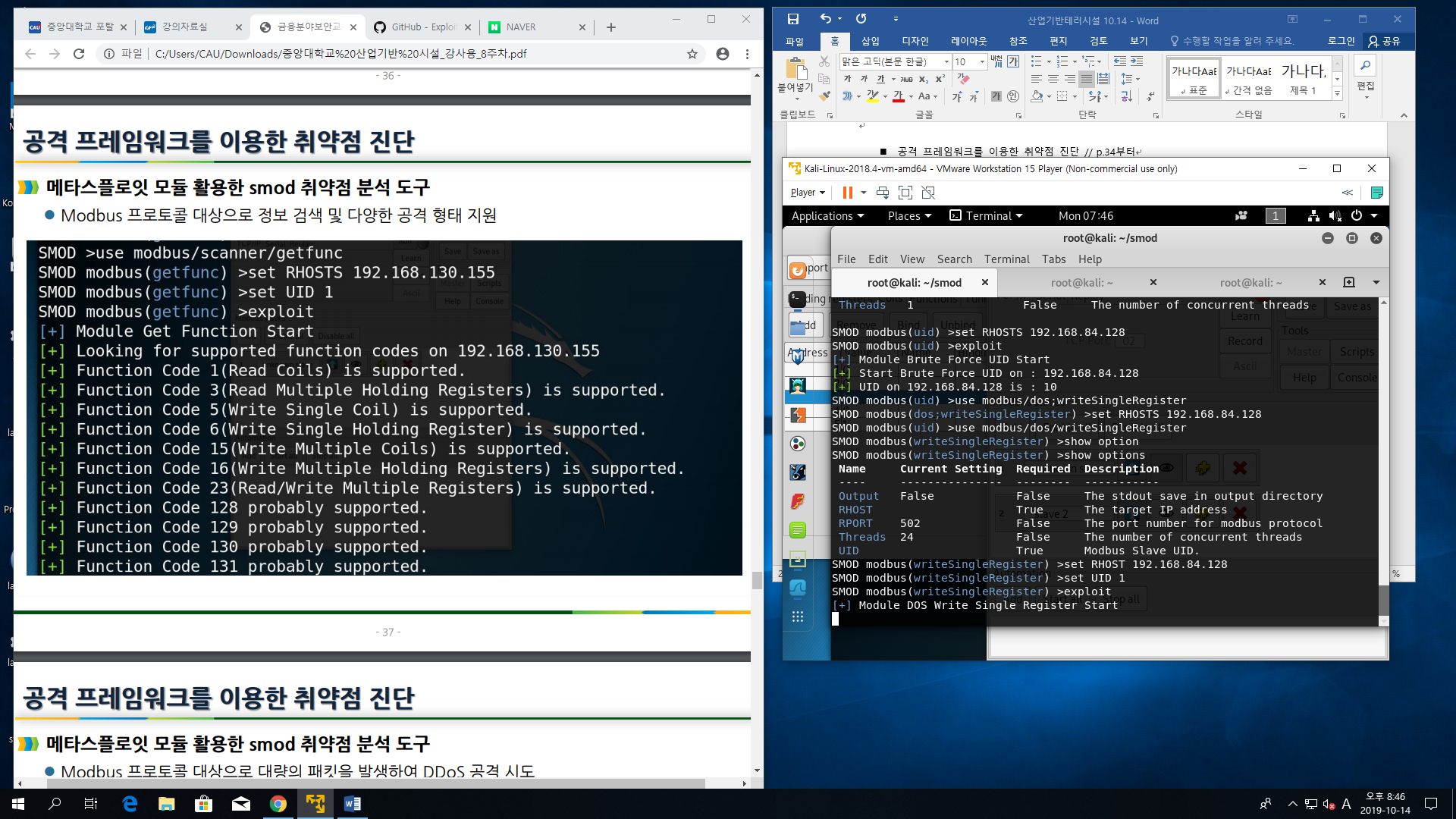
use modbus/scanner/getfunc

나가는 것 컨트롤 + z 아니면 c

Qmodmaster를 통해서 DDOS를 통한 연결이 끊겼는지 아닌지 확인 가능.

시험문제

* 구글 해킹 같은 것들의 의미들? (문제\_
* 쇼단의 옵션을 활용하는 것.(문제)
* 보안의 3대요소



정리 –

공격자 -> Modbus Slave(\*서버)

공격자 -> 웹관리자(일반적인 웹일 가능성 , HIM) 일 수도 있음. -> Modbus Slave\*(서버)

즉, 공격자는 웹관리자를 공격을해서 HIM 등을 통해서 Modbus slave에 대한 정보를 제어

관점 : 공격자가 웹관리자의 취약점을 찾아서 서버까지 공격을 할 수 있을까? 라는 것.

Docker는 클라우드 서비스랑 비슷함.

가상화 // 마음대로 추가, 삭제, 생성, 변경이 가능함.