산업 기반 시설 3,4주차

Osint : open source intelligence 공공연하게 이용가능한 소스(오픈소스)로부터 수집된 정보들

Shodan, google, naver, daum

쇼단을 통해 시스템 배너정보로부터 특정 디바이스, 컴퓨터, 라우터, 서버들의 정보

* 특정 시스템 대상으로 공격 대상을 검색할 경우 유용하게 활용

쇼단은 웹 인터페이스를 통해 사용자에게 장비에 대한 정보, 지원하는 서비스 등으로 보여줌.

직접 Nmap을 스캔하는 것보다 더 효율적일 수도 있음.

* 쇼단으로 얻을 수 있는 정보?

1. 인터넷을 사용하는 서버 및 장비의 정보 / 네트워크/서버 정보
2. 열려있는 포트 정보
3. 호스트 네임 정보 / 버전 정보

* 쇼단 기본 검색 옵션

1. City // linux city:”Seoul”
2. Country // country”KR”
3. Net // cisco net 127.0.0.1/24
4. Os // os:”ubuntu”
5. Port // port:”502”
6. Title // title:”naver.com”
7. Product // product:”cisco”
8. Org // webcam org:”Korea Telecom”

* 쇼단 웹사이트에서 산업 기반 시설에 대한 검색 활용 // siemens s7 102 / modbus 502

Slave ID Data – 각 도메인의 unit ID가 나옴

Hostname:”naver.com” – 특정 도메인이 들어가 있는 정보검색 // title과 비교해봐야함.

Net:”74.125.23.0/24” – 서비스 ip대역 c클라스 범위 검색

“MongoDB Server Information” port:27017 -autentication – 몽고db중에서 인증이 되지 않은 서버 검색

All:”mongodb server information” all:”metrics “ – 몽고디비 결과에서 도출되는 문자열을 기준으로 검색

Webcam country:”KR” org:”korea telecom”

Title:”Outlook Web Access” !port:”443,80 – 아웃룩 웹 페이지 접근 중에서 443, 80포트를 제외한 서비스 검색

“230 Login Successful” Port:”21” // 포트에 따옴표 유무 해보기 – 21번 포트를 사용하는 ftp서비스에서 로그인이 성공한 사례 검색

Port:21 Anonymous user logged in – ftp 서비스 중에 21번포트에서 익명으로 연결되는 서버

Port:”80” has\_screenshot:”true” – 80번 포트중에 스크린샷이 저장된 정보 검색

* 쇼단을 통한 침해사고 사례

1. 쇼단에 노출된 몽고유 공격 – 데이터베이스의 락을하여 사용못하게 한 후, 비트코인 요구

랜섬웨어 형태의 공격에 감염되었다. 하루 27000개 이상 – 공격하는데 13초 소요