산업기반 테러 시설 첫번째 동영상

마인크래프트와 같은 경우 서버가 굉장히 많이 열려있다.

Top voted에 webcam, cam과 같은 태그들을 클릭하면,

Industrial control systems에는 외부에서 사용하고 있는 포트들이 열려있다.

접근제어와 보안이 안되어있는상태의 포트에 접근이 가능하다.

대표적 프로토콜 modbus / siemens / dnp 이다. / 표준처럼 사용하고 있음.

모드버스는 502라는 프로토콜을 사용한다.

Slave ID Data : 컴퓨터에 서버로 동작/ 사용자가 마스터라는 것으로 붙음 / plc프로그램과 연결이 되어서 여기서 동작이 되어서 제어가 가능하다.

즉, 외부에서 포트가 열려있는경우 공격자가 제어를 할 수 있다.

모드버스는 slave id data라는 것으로 검색을 해서 정보를 얻을 수 있다. // 모드버스라고 검색해도 나옴. 이런식으로 관련된 포트들이나 문자열을 쇼단에서 활용할 수 있다.

94p 장표 : 산업기반시설 프로토콜 포트이고 siemes 는 102 / simatic 161번

이러한 포트들을 쇼단이나 이런 것을 통해 검색할 수 있다. 이런정보들이 노출되어있기 때문에//

95p 장표 : 프로토콜별 발생 취약점 // 취약점들이 노출된 것을 볼 수 있다.

10점 만점에 10점이 젤 위협적이다. // 만약, 포트가 열려있다. 그러면 공격기법들을 사용해서 공격을 진행할 수 있다.

vnc has\_screenshot:”ture” 라고 검색하면 프로토콜과 관련된 산업기반 (스카다 시스템)

즉, vnc 5900포트 쪽에 접속을 한다음에 여기서 사용자들이 사용할 수 잇는 프로그램에 접속을 해서 여기에서 접속을하면 각각 프로토콜로 장비들에게 날라간다.

즉, 프로토콜이 노출이 되면 각 장비들도 노출이 된다.

Ics has\_screenshot:”true” // ics장비쪽에 관련된 화면들이 노출되는 것을 볼 수 있다.

🡪 쇼단을 이용해서 어떻게 다양한 정보들을 획득할 수 있는지 ?!