Smart Grid-en Zibersegurtasuneko laborategia

Smart Grid-en Zibersegurtasuneko laborategiak, Lehen mailako banaketa-subestazioa batetako komunikazioetako Software-Hardware ingurunea antzeratzen du, non subestazio elektriko baten ekipamendu elektrikoak (interruptoreak, transformadoreak…) kontrolatzen eta superbisatzen duten ekipamendu elektronikoak (IED) zabaldu dira. Halaber, subestazio ekipoetara konektatzen den, oinarrizko funtzioak dituen Kontrol zentroa simulatzen da Laborategiak aukera ematen du honako hau egiteko: - Kontrol-zentroaren eta azpikuntzaren ekipamendu eta sistemen arteko benetako komunikazioa simulatzea. - Sartze probak sortzeko tresnen bidez (hacking etikoa), zibererasoen multzoa erreproduzitu - Eraso horien aurre, ekipoen (RTU, SCU, babes releak, …) eta kanpoko fabrikatzaileen Informazio sistemen (SCADA, servidor LDAP, …) erantzuna probatu - Kanpoko fabrikatzaileek garatutako erasotzeko detekzio tresnen eraginkortasuna frogatu. - Ingurumen biak (subestazioa eta Kontrol zentroa) bi routeren artean ezarritako Ethernet sare baten bidez konektaturik daude. Horrek kanpoko sarreren kudeaketa ahalbidetzen du. Router biek VPN konexioa ezartzen dute

EKIPO ETA OSAGAI GARRANTZITSUENAK

- **Kontrol Zentroa**

Laborategiak bi ingurune dauzka, Kontrol Zentroa ingurune horretan SCADA instalaturik dagoena, sare elektrikoaren funtzionamendua simulatzen duena (subestazioara murriztua), eta Subestazio ingurunea. Bertan, ekipo elektronikoak instalaturik daude (SCU eta Babes Releak) KONTROL ZENTROKO OSAGAIAK - Router: Subestazioko router-arekin VPN konexioa ezartzea ahalbidetzen du - Internal switch: Kontrol Zentroko ekipo guztiak konektatzen ditu - SCADA Ekipoa. Subestazioaren kontrola eta monitorizazioaren softwarea dauka (SCADA). Halaber, Kontrol Zentrutik IED-en konfigurazioaren aldaketa egitea ahalbideratzen du. - LDAP y NTP Ekipo Zerbitzuak : Ekipo honek subestazioko IED-tik sartzen diren zerbitzari desberdinak ditu barne - Zerbitzuak exekutatzen diren zerbitzaria: o LDAP: IEDS-ei, erabiltzaileen eta informazio sistemen kontrol, sarbidea (autentifikazioa eta baimena) egiten die o NTP: Denboren sinkronizazio zerbitzua ematen du

- **SecureGrid Hacking Tool Box (HTB)**

  SecureGrid Hacking Tool Box (HTB) subestazio elektriko baten gailu elketronikoetara sartzen eta konfiguratzen usten duen tool box bat da. SecureGrid HTB ekipamendu fabrikatzaileek erabil dezaten eginda dago, beraien ekipoek eskaintzen duten segurtasun maila ziurtatzeko.

- **SOTER**

  Subestazio elektriko eta industria instalazioen anomalien monitorizazioa.

- **Subestazioa**

  Laborategiak bi ingurune dauzka, Kontrol Zentroa ingurune horretan SCADA instalaturik dagoena, sare elektrikoaren funtzionamendua simulatzen duena (subestazioara murriztua), eta Subestazio ingurunea. Bertan, ekipo elektronikoak instalaturik daude (SCU eta Babes Releak) SUBESTAZIO EKIPAMENDUA: - Router: Subestazioko router-arekin VPN konexioa ezartzea ahalbidetzen du - Subestazioko Kontrol Unitatea: Telekontrol protokoloaren IEC 60870-5-104 bidez kontrol-zentroaren SCADA-rekin komunikazio bat ezartzen duen urruneko unitatearen funtzioak betetzen ditu. Onartu dezakeen beste protokolo batzuk Modbus TCP etal DNP3-TCP dira. Bestaldetik, Modbus TCP y el DNP3-TCP protokoloaren bidez, Babes Rele-en 61850 bezeroaren funtzioak betetzen ditu baita ere - Switch Industriala:IED guztiak konektatzen ditu Subetazioko BUS-a ezarriz. - Babes Releak: Ekipo elektrikoen babes funtzio betetzen ditu (interruptoreak, transformadoreak,…). Rele hauek IEC-61850 protokoloa ezartzen dute, honek ahalbideratzen du: OMICRON-CMC 850 ekipoek sortutako seinale elektrikoak jasotzea, SCU-rekin komunikatzea eta beraien artean GOOSE bialtzea - Elikatze iturriak: Elikadura etengabea duten errelek (Vcc) dagokien elikatze iturriekin horniturik daude. - SCADA ekipoa. Subestazioaren kontrola eta monitorizazioaren softwarea dauka (SCADA). Halaber, Kontrol Zentrotik IED-en konfigurazioaren aldaketa egitea ahalbideratzen du. - OMICRON – CMC 850: 3 Merging Units simulatzeko aukera ematen du, subestazioko datu elektrikoak eskuratzeko ekipoak. Ekipo hau TCP / IP bidez babes erreleetara konektatzen da Subestazio Bus-aren bidez. - OMICRON –

CMC 256: Seinu elektrikoak simulatzeko eta sarrera eta irteera digitalen konexioen bidez babes-releetara zuzenean konektatzeko aukera ematen du.

- **WHITEZONE**

  WHITEZONEk malware presentzia eragozten du instalazio industrialen eremu operatiboan, eremu mugatu gisa diseinatutako eremuetara software segurua eta identifikatua garraiatzen duten baimendutako erabiltzaileei sarbidea murriztuz. Hau, industria gunea ziurtatzeko eta produkzio industrialeko kontrol-gailuak eguneratzeko prozesua hobetzeko era bat da • USB-ren bidez eremu operatiboan erabiliko den informazioa ziurra dela ziurtatzen du, hau da, ez dagoela birusik edo malware-rik. • Eskuz edo NFC txartelaren bidez erabiltzaileak egiaztatzen ditu - Babestutako eremuan erabiliko diren datuak hautatzeko aukera ematen du eta aztertzen ditu birus edo malware edota baimendu ez den daturen bat bilatzeko multi-birus odeian dagoen zerbitzari baten bidez. Egiaztapen hau gaindituz gero "USB Whitezone ©" tekla agertzen da eta bertan sinaturiko eta enkriptaturiko datuak kopiatuko dira. Horrela ezin izango da aldaketarik egin. USB Whitezone © horiek babestutako eragiketen eremuan, balioa izango duten bakarrak izango dira. Honez gain, osagai honek denbora errealean bidaltzen du bere jarduera software backend-era. • Software agentea instalatutako ordenagailuko USB portuaren jarduera guztia kontrolatzen duen elementua da. Whitezone © USB ez den gailuren bat sartzen bada, berehala kanporatuko da bere erabilpena ezinezkoa izanik. USB Whitezone © bat konektaturik badago bere edukia aldatu ez dela egiaztatzen du. Aldaketarik egon bada, USBa berehala kanporatzen du. Software agenteak backen-eri bere jarduera guztia (denbora errealean) komunikatu diezaioke.

APLIKAZIO-EREMUAK

Aktiboen babesa
Erasoen aurreko erantzuna
Erasoen detekzioa
Mehatxu eta arriskuen identifikazioa

AKTIBOAK ESKAINTZEN DITUEN ZERBITZUAK

Benetako komunikazioen simulazioa kontrol zentroen eta azpiestazio elektrikoen artean ziberdefentsa xedearekin

Benetako komunikazioen simulazioa kontrol zentroen ekipo eta sistemen eta azpiestazio elektrikoen artean, ziberdefentsa probak egin ahal izateko, fabrikatzaile ezberdinek garatu dituzten tresnek erasoak antzemateko duten gaitasuna probatu ahal izatearren.

Benetako komunikazioen simulazioa kontrol zentroen eta azpiestazio elektrikoen artean zibererasoen aurrean

Benetako komunikazioen simulazioa kontrol zentroen ekipo eta sistemen eta azpiestazio elektrikoen artean. Horren xedea da erasoen aurrean fabrikatzaile ezberdinen ekipoek (RTU, SCU, babes erreleak…) eta informazio sistemek (SCADA, LDAP zerbitzaria…) ematen dituzten erantzunak probatzea ahalbidetzen dituzten zibereraso probak egin ahal izatea.

Zibersegurtasun industrialeko entrenamendua segurtasun operadoreentzat eta hacker etikoentzat

Hacking etikoa egiteko tresna multzo baten erabilpena, zibereraso mota ezberdinak simulatzen dituztenak (DoS, Man in the Middle edota kredentzialen lapurreta, besteak beste).

Zibersegurtasuneko proba funtzionalen ingurunea

Zibersegurtasuneko gaurko arauetan eskatzen diren zibersegurtasun gaitasun berrien baliozkotzea, esate baterako IEC 62351, IEE 1686 edota IEC 62443.

I DUEN ERAKUNDEA

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

FUNDACIÓN TECNALIA RESEARCH & INNOVATION
Harremanetarako pertsona:
Ana Isabel Ayerbe Fernandez-Cuesta