14.12

<http://elektrokem.hr/ek-sustavi/cijena/opcenito-o-scada-sustavu>

<https://ieeexplore.ieee.org/document/7745468>

naišao sam na informacije o jednom od poznatijih SCADA honeypota (CONPOT)

<https://conpot.readthedocs.io/en/latest/concepts/file_system.html>

jako korisno!! (kako omogućiti rad sa datotekama i podatcima na sistemu gdje trebamo ograničiti mogućnosti napadačima bez da bude pre očito da je sistem honeypot)

* naredbe kao chmod() moraju biti onemogućene ali ftp callovi nekad koriste te naredbe

15.12

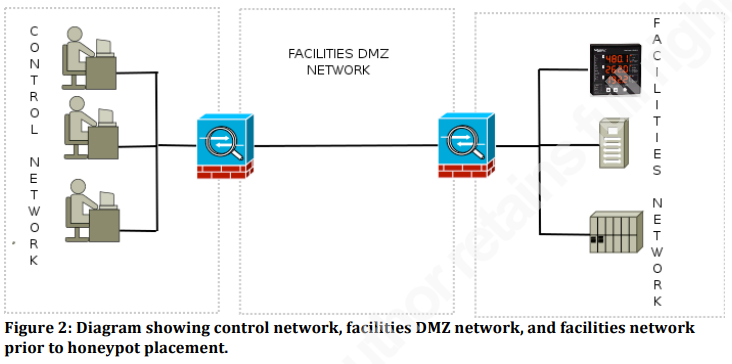
<https://www.giac.org/paper/gcia/8775/designing-implementing-honeypot-scada-network/112185>

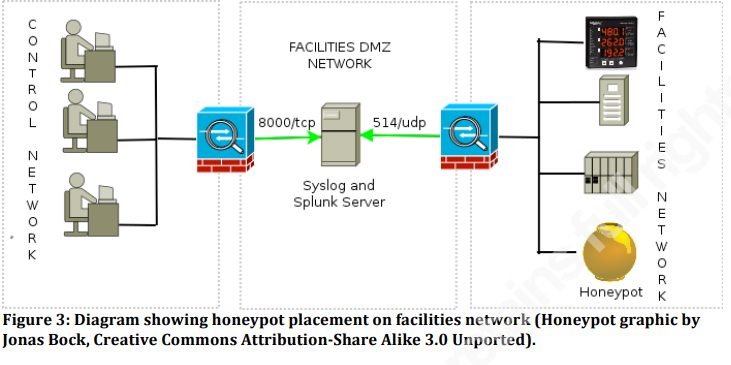
* nakon istrazivanja o prednostima stvaranja honeypota kao SCADA sustav je da ga mozemo konfigurirati da izgleda bilo kako a ne samo kao osnovni server na linuxu ili windowsu. Mozemo predstaviti sustav napadaču kao sustav za kontrolu temperature ili hlađenja
* druga prednost je što ne blokiramo nikakav promet prema ovakvom sustavu pa je manja mogućnost od greške prvog tipa ali može se kontrolirati ako to želimo sa honeywallom

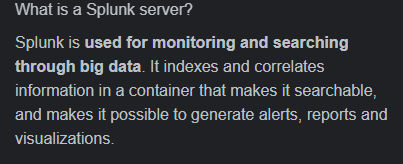
16.12

dobar honeypot treba oponašati znacajke sustava na kojem se porkreće kako bi izgledalo vjerodostojno

podrška je također iznimno važna za dobar honeypot

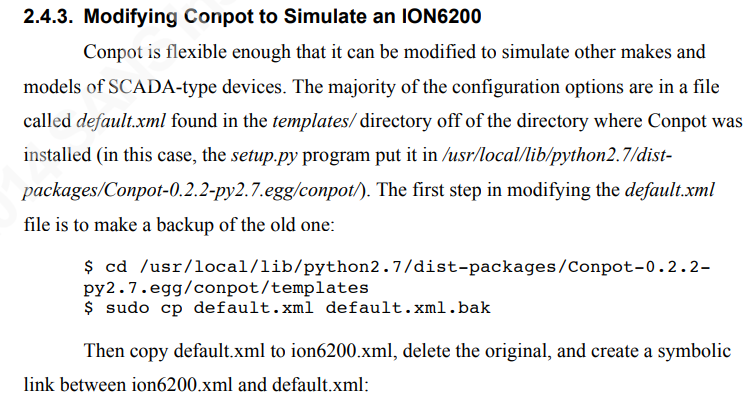






17.12

u zadnjem linku postoje upute kako instalirati honeypot server i kako oponašati rad nekih SCADA sustava



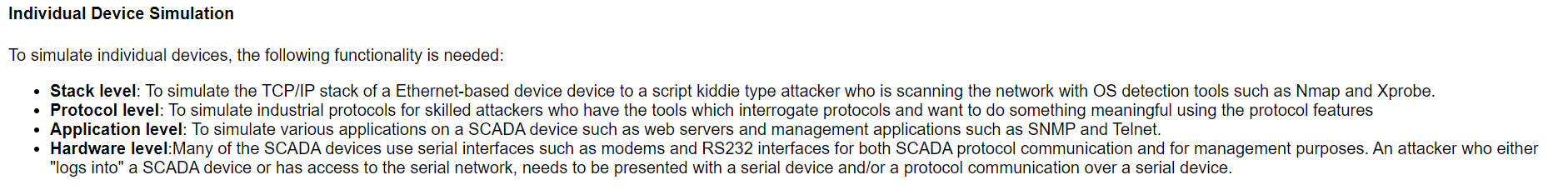
(str 15)

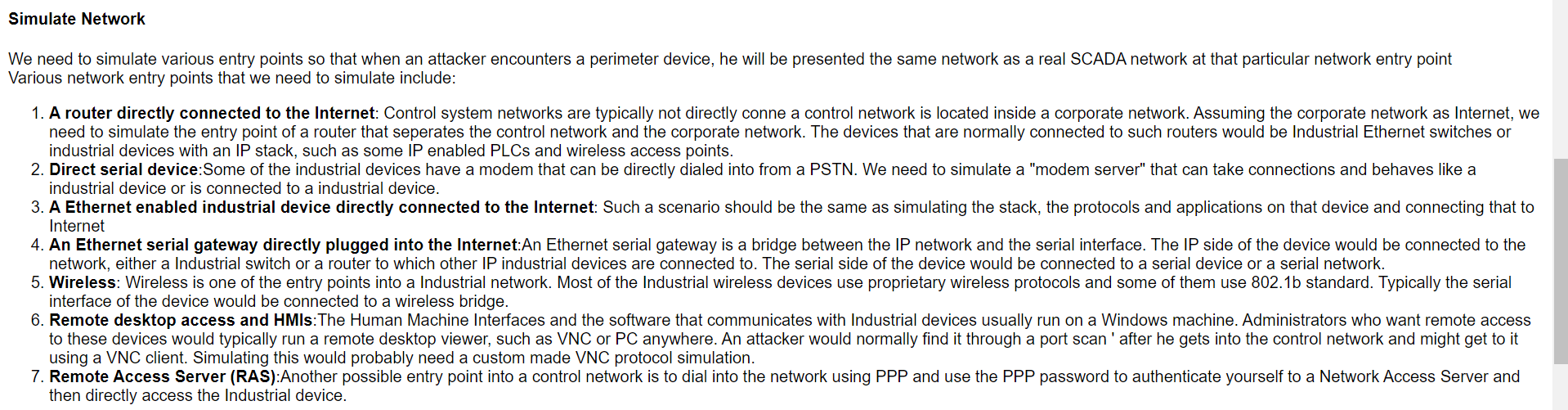
još jedna dobra implementacija sustava bi bila da nam uz cuvanje logova server dojavljuje kada ima prometa na nasem honeypotu

18.12

honeypot u scada sustavima možemo podesiti da oponašaju pojedini uređaj ili cijelu mrežu

to se radi na sljedeći način





<https://www.youtube.com/watch?v=EIdjW4VgbA4>

odličan video o tome kako se gradi SCADA Honeypot