Dizajn sustava za poučavanje

Dizajn ovakvih sustava je utoliko lakši što se od korisnika (tj. napadača) očekuje “pristojno” ponašanje – sustav postoji kako bi korisnik mogao nešto naučiti u sigurnom okruženju, te nema potrebe za većom razinom izolacije (poput onemogućavanja izlaznih veza). Moglo bi se reći da se korisniku naivno vjeruje, ali unatoč manjoj razini izolacije, potrebno je pratiti sve pokrenute naredbe i sav mrežni promet.

Kao i u dijelu o dizajnu sustava za automatsku evaluaciju tehnika napada, prvo se odabire virtualna ili fizička implementacija. Potom se omogućuje nekoliko ranjivosti koje su pod nadzorom (zna se koliko je sustav moguće kompromitirati), ali nije potrebno pratiti način iskorištavanja ranjivosti. Osim ranjivosti tog tipa, moguće je korisniku pružiti i ranjivosti lokalnog tipa – nakon što dobije korisničku ljusku iskorištavanjem ranjivosti “izvana”, da bi stekao veće privilegije mora iskoristiti i neke lokalne ranjivosti. Ovakav sustav je moguće osmisliti da bude kao “zabavni park” korisniku, i moguće je napraviti skup zadataka (poput igre) koje korisnik mora izvršiti, prelazeći s jednog nivoa na drugi. Ukoliko bi taj sustav koristio veći broj korisnika, tada je izolacija sustava prema van (odnosno zabranjivanje izlaznih veza) poželjna, jer je teško kontrolirati svakog korisnika. No, u slučaju da je to sustav koji se koristi interno na nekom tečaju unutar lokalne mreže, nije potrebno ništa izolirati jer je vidljiva samo lokalna mreža unutar koje se sustav nalazi, a u toj lokalnoj mreži bi se nalazili samo ranjivi sustav i svi polaznici tečaja.