Ofenzivna sigurnost

Laboratorijska vježba  
Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva

NAZIV LABORATORIJSKE VJEŽBE

IME I PREZIME

Zagreb, dd. mjesec godina

# Uvod (do 1000 znakova)

Kratki uvod koji daje kontekst, tj. potrebu i važnost toga s čim se bavi laboratorijska vježba. Primjerice:

* ako je potrebno demonstrirati alat za MITM napad, onda u uvodu treba malo raspisati potrebu za MITM napadima.
* ako se demonstrira alat za istraživanje informacija (reconnaissance) tada se piše o značaju istraživanja

Neke napomene:

* Nemojte kao naslov stavljati ime alata, naslov mora reflektirati zadatak koji se rješava.
* Možete dodavati potpoglavlja po potrebi
* Cijelo izvješće ne bi smjelo preći 10 stranica, brojeći sve stranice!

Vrlo bitna napomena: iako je naveden broj znakova po poglavlju, to je u ovom trenutku samo gruba procjena i prilagođavat će se sa iskustvom. Međutim ono čega se svakako morate držati, i što se neće mijenjati, je:

* Izvješće mora biti jasno i kompletno.
* Treba paziti da su poglavlja dobro balansirana! Karikirano, nema smisla napisati uvod od 5 strana i onda na jednu stranu „stisnuti“ sve ostalo.

# Zadatak (do 1000 znakova)

Konkretni zadatak koji je potrebno riješiti. Treba osmisliti nekakvu situaciju u kojoj se treba koristiti alat koji je cilj vježbe. Treba eksplicitno napisati da se koristi specifičan alat, tj. to je dio zadatka. Primjerice,

* ako je potrebno pokazati korištenje alata mitmproxy, onda se može složiti priča o nekakvom trenutku u kojemu napadač treba otkriti nekakve podatke praćenjem mrežnog prometa te se potom sugerira korištenje alata mitmproxy.
* u slučaju istraživanja (reconnaissance) treba osmisliti scenarij u kojemu se traži istraživanje nečeg specifičnog, neke organizacije

# Teorijski podloga (do 4000 znakova)

Opisuje se tehnička pozadina cijele vježbe. Vodite računa da studenti u laboratorijskim vježbama trebaju koristiti znanja koja dobiju na predavanjima, ali isto tako da trebaju dodatno istražiti nekakve dodatne materijale. To sve treba pisati u rješenju vježbe. Zato nemojte ovdje opisivati sve u detalje. Primjerice,

* u slučaju mitmproxy alata opisuje se protokol koji se presreće te način kako se može doći u MITM situaciju. Također, opisuje se ukratko alat koji se koristi kao i neke njegove osnovne tehničke karakteristike
* u slučaju alata za istraživanje treba ukratko navesti i opisati izvore informacija – posebno one koji se koriste u laboratorijskoj vježbi. Također, kratko opisati sam alat koji se koristi.

# Postavke za vježbu (do 5000 znakova)

Opisuje se okolina u kojoj se postavlja zadatak te u kojoj će se rješavati zadatak. Opis treba biti takav da svakome omogućava repliciranje okoline za vježbu. Nije nužno ići u opisu do najsitnijih detalja, može se u nekom trenutku samo napisati **što** je potrebno napraviti, ne i **kako**.

Primjerice:

* za MITM napad, složiti računalo žrtve i poslužitelja s kojim komunicira, te računalo napadača. Sve to je potrebno spojiti. Za računalo napadača može se koristiti distribucija Kali. U opisu, dovoljno je reći da se koristi Kali, eventualno s popisom dodatnih paketa koje treba instalirati, ali se ne mora za svaki paket detaljno raspisivati instalacija.
* u slučaju alata za istraživanje, ako je to sve što je potrebno, dovoljno je napisati da se instalira distribucija Kali te kako se sam alat pokreće. Eventualno, ako je potrebno nešto doinstalirati – uključivo sam alat – treba to također napomenuti.

# Rješenje vježbe (do 5000 znakova)

Opis rješavanja zadatka. Opis mora biti takav da svakome omogući ponavljanje cijelog postupka rješavanja zadatka. Ovdje se ide u detalje alata, ali samo one koji su korišteni za rješavanje vježbe. Također, trebaju se istaknuti potencijalna ograničenja ili poteškoće u rješavanju zadataka.

Primjerice:

* za MITM napad treba opisati korake kroz koje je potrebno proći da se on implementira u kontekstu okruženja opisanog u poglavlju Postavke za vježbu.

# Zaključak (do 1000 znakova)

Ovdje treba ukratko napisati što se naučilo tijekom rješavanja vježbe! Treba izbjegavati iznošenje novih činjenica u zaključku!

Primjerice:

* Za MITM napad može se napisati koliko je jednostavan za provođenje te što može spriječiti napadača u provođenju napada.

# Literatura

Ovdje popišite literaturu koju ste koristili tijekom definiranja vježbe, njena rješavanja, i na kraju pisanja izvješća. Pozivajte se na pojedine reference u tekstu!