SIGURNOST OPERACIJSKIH SUSTAVA I APLIKACIJA 2021./2022.

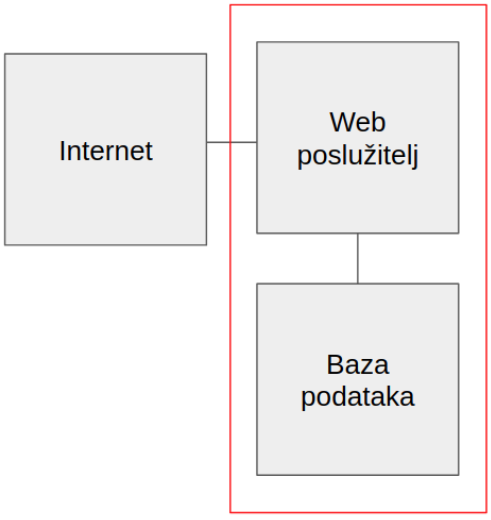
Druga laboratorijska vježba: Modeliranje prijetnji

Uvod

Jedna od vrlo važnih zadaća u kontekstu računalne sigurnosti je modeliranje prijetnji. Modeliranje prijetnji se može raditi na različite načine. Jedna od njih je pomoću vizualnog modela koji se zove **stablo napada**. (Postoji i šuma stabala napada, te graf napada.) Proučite stabla napada uz pomoć literature (slajdova s predavanja) i Interneta. Također, proučite sljedeći znanstveni rad: “Modeling Internet Attacks, *Tidwell et al.*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.108.9040&rep=rep1&type=pdf “ koji bi Vam trebao pomoći u rješevanju zadatka ove laboratorijske vježbe. U tome radu možete (između ostalog) vidjeti kako izgleda stablo napada.

Zadatak

Želimo znati kako bi napadač mogao kompromitirati **web sjedište** i koje zaštite moramo ugraditi da bismo to izbjegli. Promatrani **sustav** (web sjedište) prikazan je na sljedećoj slici (Slika 1.).



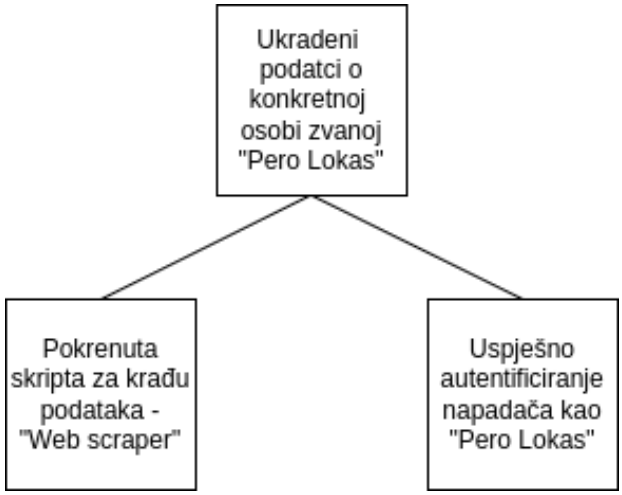
Slika 1.: Modelirani sustav (web sjedište), granice sustava označene su crvenim pravokutnikom

Na web sjedištu su dostupni osjetljivi podatci o ljudima (korisničko ime, ime, prezime, oib, mjesto rođenja, godina rođenja, jmbag, adresa prebivališta) nakon što se osoba autentificira pomoću korisničkog imena i zaporke. Neki podatci (korisničko ime, ime, prezime, mjesto rođenja) su i javno dostupni (bez autentifikacije konkretnog korisnika).

Modelirajte napadačev napad koji ima za cilj ukrasti podatke (što više njih) o određenoj osobi (primjerice, osoba se može zvati “Pero Lokas”, a njezino korisničko ime može biti peroLokas11) s modeliranog sustava - web sjedišta. (Ovo radimo u konačnom cilju razvijanja boljih zaštita.)

Preporučamo metodu preduvjeta odnosno *eng.* “preconditiona”. Odozdo prema gore, podređeni čvor je **uvjet** koji mora biti zadovoljen da bi izravni roditeljski čvor bio istinit; čvorovi djeca su odvojeni **ILI** kvantifikatorom - dovoljno je da jedan vrijedi. Slobodno odaberite i objasnite neku drugu metodu.

Vrlo **krnji prikaz** onoga što želimo da napravite u smislu veličine stabla, broja čvorova i oblika čvorova prikazan je na sljedećoj slici (Slika 2.).



Slika 2.: Primjer krnjeg stabla napada

Dakle, od Vas očekujemo - **veće razgranatije stablo** i **različite oblike čvorova**.

Upute i napomene:

1. Obratite pažnju na odabir alata za crtanje i objasnite zašto ste uzeli baš taj alat.
2. Obratite posebnu pozornost na vršni čvor (cilj) i čvorove na posljednjoj razini stabla.
3. Razmislite o korištenju različitih oblika čvorova (geometrijski likovi) i objasnite što bi koji geometrijski lik mogao predstavljati.

4. Koraci napada prikazani u stablu na Slici 2. ne moraju nužno puno kolerirati s koracima koje ćete Vi imati u vašem stablu (bitno je da je cilj isti).
5. Obrazložite koje zaštite biste uveli da biste spriječili napadačev napad. Pretpostavite da inicijalni sustav nije pokrio sve mogućnosti zaštite.

Dodatni materijali

1. Dodatne informacije o stablima napada se mogu naći na: https://www.schneier.com/academic/archives/1999/12/attack_trees.html .
2. Za korake napada kao inspiraciju možete uzeti MITRE ATT&CK https://attack.mitre.org/ .

Predaja

Dakle, potrebno je predati izvještaj koji sadrži:

1. Postupak rješavanja zadatka.
2. Konačno stablo napada.

Predajte rješenje u jednoj **pdf** datoteci. **Duljina izvještaja je ograničena** na **15 stranica A4 formata**. Preporučamo font veličine **11 pt**.

Rok za predaju vježbe je **18.5.2022.** u **23:59**. Za ispunjavanje minimuma i prolaz predmeta potrebno je poslati rješenje laboratorijske vježbe do navedenog roka (u smislu da ne pišete besmislice). Međutim, postoji **parcijalno** bodovanje laboratorija. U slučaju problema ili nedoumica prilikom izrade vježbe molimo da pravovremeno kontaktirate nastavno osoblje putem mailing liste predmeta sosa@fer.hr (isključivo koristeći fer.hr adresu).

Važno: Dozvoljeno je i poželjno diskutiranje mogućih pristupa rješavanju vježbe između studenata. Međutim, samu laboratorijsku vježbu studenti moraju raditi samostalno. Nastavno osoblje će provesti provjere sličnosti predanih rješenja, a ponašanje koje nije u skladu s Kodeksom ponašanja studenata FER-a ćemo prijaviti Povjerenstvu za stegovnu odgovornost studenata te odrediti dodatne sankcije u sklopu predmeta.