SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Autori:

Žad Deljkić, Edi Sinovčić, Katarina Ćavar, Josip Mrđen, Alen Hrga

FERsec Challenge – radionica o informacijskoj sigurnosti

Zagreb, 2017

Ovaj rad izrađen je pri Fakultetu elektrotehnike i računarstva pod vodstvom doc. dr. sc. Predraga Pale i predan je na natječaj za dodjelu Rektorove nagrade u akademskoj godini 2016./2017.

POJMOVNIK

Reverzno inženjerstvo – pojam koji predstavlja procese izvlačenja informacija ili dizajna iz izvršnog programa.

CTF – „Capture the flag“ tip natjecanja gdje sudionici moraju prvi riješiti zadatak da bi dobili tajni kod čijim unosom u sustav dobivaju bodove ili otključavaju sljedeći zadatak.

Exploit – program, podaci ili niz naredbi koji iskorištavaju ranjivost sustava

x86 – arhitektura procesora bazirana na *Intel 8086 CPU* i njezinim *Intel 8088* varijantama.

Assembly – izvršni kod programa.

x64dbg debugger – program koji služi za čitanje izvršnog (strojnog) koda.

API/ABI operacijskih sustava – sučelje operacijskog sustava, odnosno set funkcija koje nudi operacijski sustav za manipuliranje podacima i procesima.

Stack-based buffer overflow exploit – vrsta napada u kojem je cilj prepisati memoriju kojoj ne bismo trebali imati pristup.

Shellcode – jedna ili više instrukcija korištenih za iskorištavanje ranjivosti nekog programa.

OWASP Top 10 – najčešćih 10 vrsta napada na sustave. (*Open Web Application Security Project*)

SQL Injection – vrsta napada u kojoj napadač pokušava iskoristiti ranjivost baze podataka.

Command Injection – vrsta napada u kojoj napadač pokušava izvršiti naredbe na operacijskom sustavu kroz ranjivu aplikaciju ili program.

XSS (Cross-site scripting) – vrsta napada u kojoj napadač pokušava pokrenuti skriptu na korisnikovom web pregledniku.

Unvalidated Redirects and Forwards – vrsta napada u kojoj napadač pokušava manipulirati adresom na koju se aplikacija preusmjerava.

Vatrozid (Firewall) – uređaj ili program čija je namjena filtrirati promet koji dolazi ili dolazi s računala.

Sadržaj rada

1. UVOD

Informacijska sigurnost danas predstavlja sve bitniji segment u radu informacijskih sustava. Pravilno dizajnirani sustavi s naglaskom na sigurnost, osiguravaju ne samo pravilan rad sustava, već i ispravno korištenje osjetljivih korisničkih podataka koji su podložni curenjima čak i u velikim međunarodnim kompanijama, odnosno njihovim informacijskim sustavima, čemu smo svakodnevno svjedoci.

Cilj ove radionice je bio podignuti svijest o svim elementima koje jedan siguran i pravilno izrađen sustav mora sadržavati. Kako bi se sustavi mogli zaštititi, treba poznavati ofenzivnu i defenzivnu stranu sigurnosti. S obzirom na navedeno prošli smo sva poglavlja koje jedna radionica informacijske sigurnosti treba sadržavati.

Da bi sudionici u potpunosti razumjeli obje strane, onu ofenzivnu i defenzivnu, u prvom dijelu prošli smo „reversing“ tehnike i načine neutralizacije „malware“-a, a nakon toga i pisanje „exploita“, odnosno iskorištavanja samih manjkavosti u sustavu. U drugom dijelu, pričali smo o Web i mobilnoj sigurnosti, te statičkoj analizi koda.

Sudionici su dobili kompletan uvid u ono što sigurnost u realnom svijetu danas predstavlja, na pravim primjerima iz prakse. U tome su nam pomogli naši partneri iz industrije. Cilj radionice je postignut, tim više što su studenti rješavali konkretne probleme koji se stvarno pojavljuju u velikim tvrtkama.

Radionica je svojim sadržajem nadopuna kurikulumu Fakulteta elektrotehnike i računarstva. Da ovo područje u mnogočemu zanima studente, vidljivo je po njihovom odazivu na radionicu.

2. OPĆI I SPECIFIČNI CILJEVI RADA

Temelj za razvoj projekta nastao je u zajedničkoj suradnji studenata Fakulteta elektrotehnike i računarstva i profesora na fakultetu iz područja sigurnosti, kriptografije i forenzike.

Opći cilj projekta je potaknuti studente na samostalan rad i učenje u području informacijske sigurnosti, izvan okvira, ali kao nadopuna nastavnom planu i programu.

Specifični cilj projekta je poboljšati stručne vještine i steći nove kompetencije potrebne na tržištu rada. Kroz predavanja, praktične zadatke i diskusiju polaznici će: steći znanje potrebno za održavanje sustava sigurnosti u organizacijama, razumjeti programsku potporu za dubinsku analizu podataka, razumjeti metode traženja ranjivosti i načine na koje napadači iskorištavaju ranjivosti, naučiti koji su sigurnosni rizici u mobilnim aplikacijama (kako ih otkriti, spriječiti i kako se iskorištavaju), naučiti koji su sigurnosni rizici u web aplikacijama (kako ih otkriti, spriječiti i kako se iskorištavaju) te upoznati načine zaštita web stranica.

3. METODE I PLAN RADA

Organizacija radionice počela je u listopadu 2016. godine. Prva faza organizacije je bilo predstavljanje ideje o radionici i formiranje organizacijskog tima. Zbog kompleksnosti organizacije bilo je potrebno dodijeliti specifične uloge svakom pojedinom članu.

Uloge su bile:

- FR (*Fundraising*) koordinator - zadužen za komunikaciju i sastanke s predstavnicima iz industrije
- PR (*Public Relations*) koordinator - zadužen za promociju radionice među studentskom populacijom na fakultetu i društvenim mrežama
- Akademski koordinator - zadužen za kreiranje i održavanje kvalitete sadržaja predavanja
- Koordinator za logistiku - zadužen za logističke probleme organizacije, osiguravanje letaka, plakata, komunikaciju s dizajnerima te osiguravanje potrebnih resursa tijekom radionice
- Glavni koordinator - zadužen za koordinaciju tima, održavanje sastanaka, konzistentnosti u toku informacija te komunikaciju s predstavnicima fakulteta

U početnoj fazi organizacije su određeni rokovi za početak promocije i odnosa s predstavnicima industrije, okvirni termin radionice i prijedlog akademskog dijela, odnosno sadržaja predavanja.
PR radionice trajao je od prosinca 2016. godine do kraja radionice, a uključivao je objave na društvenim mrežama, izradu promotivnih videa koji su se prikazivali na video zidu Fakulteta elektrotehnike i računarstva te podjelu letaka na prostorima fakulteta.
FR radionice je počeo u studentom 2016. godine i uključivao je sastanke s predstavnicima industrije u svrhu prikupljanja prijedloga za akademski dio i sredstava za održavanje radionice.
Posao akademskog koordinatora bio je izrada konceptualnog rasporeda predavanja i pripremanje infrastrukture i zadataka za natjecanje koje se održalo na završetku radionice. Uz to, akademski koordinator je, u suradnji s profesorima, bio zadužen za kreiranje pred-ispita kojim su se provjeravala potrebna predznanja prijavljenih studenata.

Termin održavanja radionice bio je 18.3.2017.-26.3.2017.

4. REZULTATI

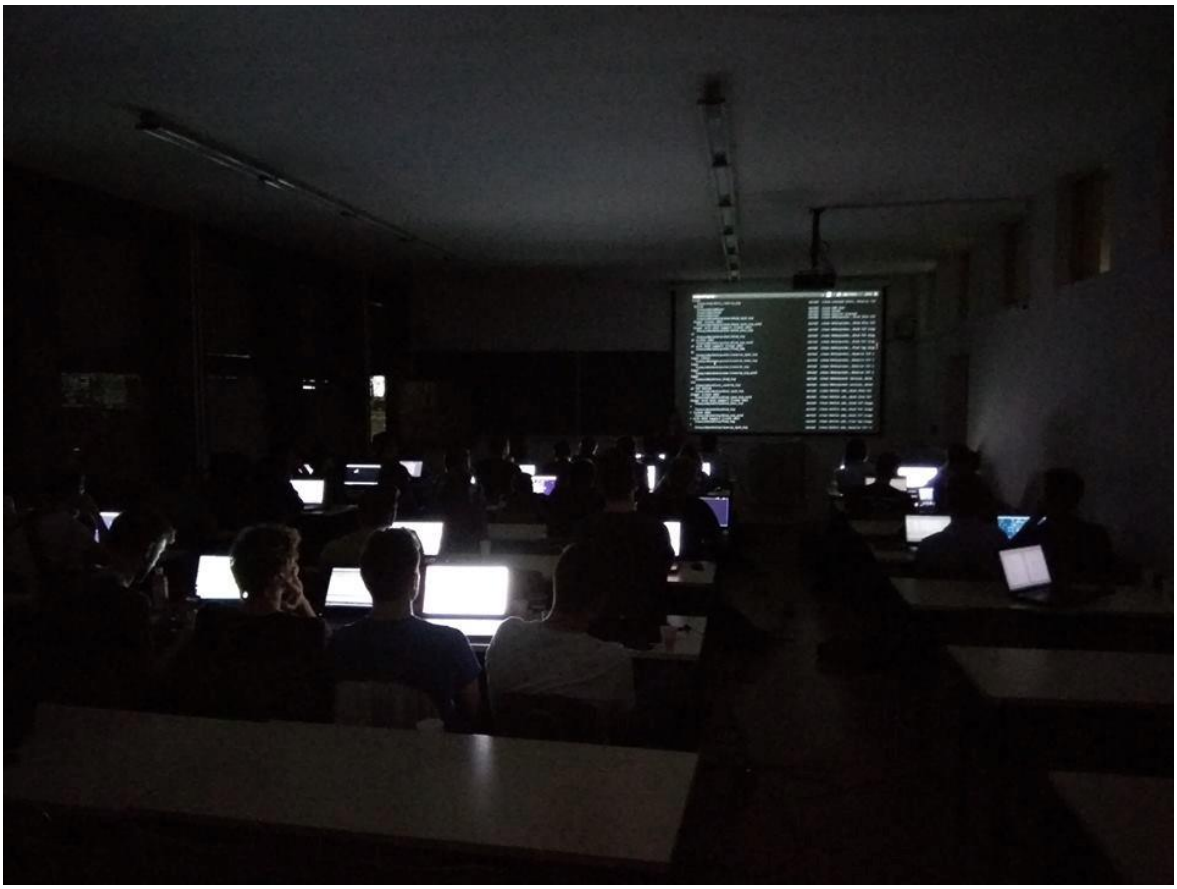
Radionica je trajala osam dana po četiri sata dnevno, a teme su bile (s kratkim opisom):

Prvo predavanje (18.3.):

Uvod i osnove reverznog inženjerstva. Osnovno razumijevanje x86 assembly-a i upoznavanje s x64dbg debuggerom.

Drugo predavanje (19.3.):

API/ABI operacijskog sustava. Osnove anti-debug i anti-dissasembly metoda i pakiranja. Naprednije korištenje x64dbg debuggera i pregled ostalih alata za reverzno inženjerstvo.



Slika 1. Pregled alata za reverzno inženjerstvo

Treće predavanje (20.3.)

Koncept ranjivosti i njihovo iskorištavanje u praksi. Razvoj stack-based buffer overflow exploita. Prepisivanje lokalnih varijabli, prepisivanje povratne adrese te zapisivanje shellcode-a i skokovi na shellcode.

Četvrto predavanje (21.3.)

Uvod u tehnike otežavanja/zaštite od exploita (NX, ASLR, stack canary) i načini zaobilaženja. Razlika između lokalnih i udaljenih exploit-a, korištenje de Bruijn niza, uvod u fuzzing.

Slika 2. Slike s četvrtog predavanja

Peto predavanje (22.3.)

Ofenzivna web sigurnost, praktične primjene i uvod u OWASP Top 10 načina napada na web aplikacije. Naglasak je bio na SQL i command injectionu te ubacivanje skripti u web stranice (XSS - Cross-site scripting). Neadekvatna zaštita podataka te neprovjereno preusmjeravanje na zloćudne web stranice (Unvalidated Redirects and Forwards).

Šesto predavanje (23.3.)

Defenzivna sigurnost, osnove zaštite aplikacija i sustava. Upoznavanje s konceptom vatrozida i primjenom tehnologije F5 Web Application Firewall.

Sedmo predavanje (24.3.)

Uvod u mobilnu sigurnost. Upoznavanje s najčešćim ranjivostima mobilnih aplikacija te načinima kako ih iskoristiti. Čitanje i analiza Android aplikacija te upoznavanje s alatima koji se koriste za njihovu analizu.

Osmo predavanje (25.3.)

Statička analiza koda, sustavi i alati u primjeni. Upoznavanje s tehnologijom Checkmarx.

Slika 3. Sudionici s organizatorima na kraju radionice

Slika 4. Organizatori radionice prije početka radionice

Natjecanje „Capture The Flag“ (26.3.)

Online natjecanje na principu „Capture The Flag“ pri kojem su sudionici mogli vježbati naučeno kroz predavanja u simuliranoj okolini. Pisanje exploita, reversanje te upadi na poslužitelje (ofenzivna Web sigurnost), obrana od tih napada te reversanje i exploitanje dijela mobilne aplikacije su sve bili dijelovi koje su sudionici imali priliku iskusiti na natjecanju kako bi ono naučeno dodatno usavršili. Natjecanje je trajalo 24 sata.

5. ZAKLJUČCI

Na radionicu smo planirali primiti 30 studenata, ali smo zbog velikog interesa primili njih 47. Razlog tome su 73 prijave te kvaliteta samih prijava, gdje je razlika između kandidata bila minimalna. Izniman je uspjeh što je od primljenih 47 sudionika uspješno završilo radionicu njih 43, što znači da je njih 43 sudjelovalo na barem 80% predavanja te sudjelovalo u rješavanju zadataka koji su bili prisutni na svakom predavanju. Prosječna posjećenost predavanja bila je 93%. To je izniman postotak, što govori o kvaliteti same radionice. Izrazito nam je drago što je projekt ovakvog kalibra ostvaren ove godine. Također, postoji tendencija da ovaj projekt bude inkubator promjena percepcije „hakiranja“ kao nečega negativnog te da se hakerski alati mogu koristiti za poboljšanje sustava i njihovo unaprjeđivanje. Svijest o tome uvijek kreće od akademskih krugova te smo ponosni što smo i mi dio pokreta za micanje tabua s ovog područja sigurnosti.

Kroz sve navedeno vidljivo je da je projekt u potpunosti ispunio svoje ciljeve te da slijedi dugogodišnji period kada će ovo biti centralni događaj koji promiče odgovorno, smišljeno i dobronamjerno korištenje ofenzivnih i defenzivnih tehnologija i alata u području sigurnosti.

6. PRILOZI

[1] Općenito o radionici: http://eestec-zg.hr/fersec/

[2] Materijali za predavanja: http://eestec-zg.hr/fersec-materijali/

[3] Facebook stranica radionice: https://www.facebook.com/ferseczg

[4] Medijske objave:

- http://www.netokracija.com/fersec-challenge-racunalna-sigurnost-132746
- http://studentski.hr/studenti/vijesti/buduci-inzenjeri-organiziraju-radionicu-na-temu-racunalne-sigurnosti
- http://www.bug.hr/vijesti/otvorene-prijave-studentsku-radionicu-o-racunal/159143.aspx
- http://www2.tvz.hr/2017/03/fersec-challenge-radionica/

7. SAŽETAK

FERsec Challenge je stručna radionica o informacijskoj sigurnosti koja mladim budućim inženjerima proširuje znanje i pruža uvid u problematiku područja informacijske sigurnosti. Radionica nudi mogućnost savladavanja znanja na području web sigurnosti, reverznog inženjerstva i razvoja programa koji iskorištavaju ranjivosti sustava te rješavanja zadataka u opsegu radionice uz koje će studenti moći u potpunosti ovladati novim znanjem.

Radionica se sastoji od dva dijela. Prvi dio su predavanja i primjene znanja stečenog na predavanjima, a drugi dio čini natjecanje gdje studenti mogu nova znanja primijeniti na praktičnim problemima u simuliranom okruženju. Predavanja su održali kolega Žad Deljkić te predavači iz industrije. Svako predavanje se sastojalo od teorijskog uvoda nakon kojega su studenti na svojim računalima na pripremljenim materijalima primjenjivali novostečena znanja.

Za natjecanje je pripremljeno nekoliko poslužitelja sa sustavima na kojima su simulirane razne ranjivosti i propusti koje su studenti morali naći i iskoristiti. Osim toga, pripremljen je i sustav gdje su se pratili timovi i gdje su bili postavljeni zadaci iz svih područja informacijske sigurnosti, uključujući reverzno inženjerstvo, razvoj exploit-a, web sigurnost, kriptografiju i forenziku. Zadaci nose različit broj bodova ovisno o njihovoj težini.

Opći cilj radionice je potaknuti studente na samostalan rad i učenje u području sigurnosti jer je ona prisutna u svim oblicima poslovanja na Internetu i bitan aspekt na koji uvijek treba obratiti pozornost.

Specifični cilj radionice je poboljšati stručne vještine i steći nove kompetencije potrebne na tržištu rada. Kroz predavanja, praktične zadatke i diskusiju polaznici će: steći znanje potrebno za održavanje sustava sigurnosti u organizacijama, razumjeti programsku potporu za dubinsku analizu podataka, razumjeti metode traženja ranjivosti i načine na koje napadači iskorištavaju ranjivosti, naučiti koji su sigurnosni rizici u mobilnim aplikacijama (kako ih otkriti, spriječit i kako se iskorištavaju), naučiti

koji su sigurnosni rizici u web aplikacijama (kako ih otkriti, spriječiti i kako se iskorištavaju), upoznati načine zaštita web stranica.

Ključne riječi: Reverzno inženjerstvo, exploit

8. SUMMARY

FERsec Challenge is an expert information security workshop that aims to expand knowledge of future engineers and provide insight into information security issues. The workshop offers the ability to master knowledge in the area of web security, reverse engineering, writing exploits and solving tasks within the scope of a workshop that will allow participants to master new knowledge.

The workshop consists of two parts. The first part are the lectures and the application of knowledge gained in the lectures and the second part is a competition where students can apply new knowledge to practical problems in a simulated environment. Colleague Žad Deljkić held lectures alongside lecturers from the industry. Each lecture consisted of a theoretical introduction after which the students applied their newly acquired knowledge on their computers with previously prepared materials. Several servers were also prepared for the competition with systems that simulated various vulnerabilities and omissions that students had to find and exploit. In addition, a system was prepared through which teams were tracked and tasks from all areas of information security were solved. Those areas covered reverse engineering, exploits, web security, cryptography and forensics. Tasks carry a different number of points depending on their difficulty.

The general goal of the workshop is to encourage students to work independently and enrol in the field of information security because it is present in all forms of businesses today. It’s an essential aspect present on the Internet to which attention should always be given.

The specific goal of the workshop is to improve the professional skills and to acquire new competencies needed in the market. Through lectures, practical assignments and discussions, attendees gained the knowledge needed to maintain organization's security systems. They also gained understanding of software for deep data analysis, understanding of vulnerability methods and how attackers exploit vulnerabilities. They learned which security risks appear in mobile applications (how to discover, prevent, and exploit them), learned which are security risks in web

applications and familiarized with how to protect web sites.

Keywords: Reverse engineering, exploit