Ogledni Student: Studentski radovi na nov način

Dnevnik rada

1. tjedan (4.2 - 8.2.2014.)

U prvom tjednu rada cilj je bio upoznati se sa osnovama asemblera za MS Windows operacijski sustav. U tu svrhu prošao sam seriju videa na stranici SecurityTube.net kako bi se prisjetio temeljnih stvari vezanih za asembler na MS Windows i Linux okruženju. Serije videa koje sam gledao mogu se na navedenoj stranici pronaći pod nazivima “Windows Assembly Language” i “Linux Assembly Megaprimer”.

---

2. tjedan (10.2 - 18.2.2014.)

Dosadašnji rad

Ovaj tjedan uglavnom sam se bavio proučavanjem raznih materijala vezanih za reverzni inženjering. Preciznije, većinu vremena proveo sam čitajući određena poglavlja iz knjiga “Reversing, Secrets Of Reverse Engineering” i “Practical Malware Analysis”. U poglavljima “Foundations” i “Low-Level Software” iz prve knjige naučio sam osnovne pojmove i tehnike vezane za reverzni inženjering te sam se prisjetio asemblerskog jezika. U poglavlju “Windows Fundamentals” dobio sam uvid u arhitekturu Windows operacijskog sustava te sam se polagano počeo privikavati na Windows API pošto ću se baviti analizom zlođudnih programa na tom operacijskom sustavu. U knjizi “Practical Malware Analysis” prošao sam poglavlje vezano za prepoznavanje tipičnih dijelova programskog jezika C u asembleru. Tako sam naučio kako prepoznati razne vrste petlji (for, while), grananja (if...else, switch), strukture, povezane liste te polja. Osim toga, u navedenom poglavlju upoznao sam se i sa osnovnim vrstama poziva funkcija u asembleru (engl. calling conventions). Nakon što sam prošao navedena poglavlja te dobio određene temelje iz područja reverznog inženjerstva, pribavio sam IDA Pro alat za rastavljanje (engl. dissasembler). Radi se o jednom od najpoznatijih alata za analizu asemblera te sam u poglavlju “IDA PRO” u knjizi “Practical Malware Analysis” naučio osnove za korištenje tog alata.

Daljnji koraci

U sljedećem tjednu planiram se više orijentirati na praksu. Iz tog razloga upoznati ću se sa alatima vezanima za debugging i decompile na Windows operacijskom sustavu. Kako bi dobio dobar uvid u te alate proći ću poglavlje “Reversing Tools” u knjizi “Reversing, Secrets Of Reverse Engineering”. Također, krenuti ću sa proučavanjem Olldbg debuggera te rješavati neke jednostavnije zadatke iz područja reverznog inženjeringa.

---

3. i 4. tjedan (19.2 - 5.3.2014.)

Dosadašnji rad

U ova dva tjedna rada najviše sam se bavio reverzingom jednostavnih crackme programa sa stranice "http://thelegendofrandom.com/blog/sample-page". Uspio sam proći prvih 13 zadataka te do kraja ovog tjedna planiram završiti sa zadnja dva kako je planirano u zadatku. Sav reverzing sam radio preko Ollydbg debuggera pošto se radi o jednom od najpopularnijih alata za reverzni inžinjering. Osim praktičnog dijela čitao sam o ostalim alatima koji se koriste u reverznom inženjeringu te sam isprovao besplatni verziju IDA Pro alata.

Daljnji koraci

U sljedećem tjednu planiram završiti sa zadanim tutorialima na stranici "http://thelegendofrandom.com/blog/sample-page" te se okušati u malo složenijim problemima na stranici " http://crackmes.de".

---

5. i 6. tjedan (6.3 - 24.3.2014.)

Dosadašnji rad

U posljednja dva tjedna bavio sam se najviše reverznim inžinjeringom raznih Crackme programa sa stranice http://crackmes.de/ . Do sada sam uspio riješiti 20ak Crackmea te se sve bolje snalazim u tome području. Također, prvi puta sam se susreo sa programima pisanima u Delphi programskom jeziku. Disasemblanjem tih programa dobiva se struktura asemblerskog koda koja je donekle drugačija od asemblerskog zapisa programa pisanih u C i C++ jezicima, stoga sam dio vremena proveo čitajući literaturu namijenjenu reverznom inženjerstvu Delphi programa. Tako sam se susreo sa nekim novim alatima, poput Resource Hacker i DeDe, koji značajno pojednostavljuju reverzing Delphi programa. Osim toga, započeo sam proučavati literaturu vezanu za naprednije statičke i dinamičke tehnike reverzinga iz knjige "Practical Malware Analysis". Time sam započeo sa drugom točkom plana rada gdje je potrebno proučiti tehnike analize zloćudnih aplikacija. U sljedećih nekoliko dana nastojat ću proći cijelu literaturu vezanu za nalizu kako je dogovoreno na sastanku. Nakon toga krenut ću na analizu nekih stvarnih malicioznih programa te ,nadam se da u konačnici, ponuditi i neka riješenja za njih.

---

7. tjedan (25.3 - 4.4.2014.)

Dosadašnji rad

U posljednjih tjedan dana bavio sam se naprednijima temama iz područja statičke i dinamičke analize zločudnih programa. Prošao sam dio 2(Napredna statička analiza) i dio 3(Napredna dinamička analiza) u knjizi "Practical Malware Analysis". Na kraju svakog poglavlja u knjizi nalazi se popis malicioznih programa i zadataka koje je potrebno napraviti analizom istih te sam prošao te zadatke i time po prvi

puta zakoračio u praktični dio vezan za analizu zločudnih programa. Osim toga naučio sam se koristiti i nekim dodatnim alatima vezanima za analizu malwarea (osim Ollydbg i IDApro koje sam koristio i prije). Neki od tih alata su PEview, PEid, Dependency Walker, Process monitor, Process explorer te apateDNS.

8., 9., 10. tjedan (5.4. - 29.4.2014.)

Dosadašnji rad

U posljednja tri tjedna bavio sam se analizom stvarnog malwarea. Program sam pronašao putem stranice http://www.malwareblacklist.com/ i sudeći po podacima sa stranice VirusTotal.com , pretpostavljam da se pojavio početkom 2013. godine. Odlučio sam napisati blog post na engleskom koji sadrži detaljnu statičku i dinamičku analizu nad zloćudnim programom jer smatram kako bi neke stvari u tom postu mogle poslužiti ostalima koji se bave ovim područjem. Blog sa detaljnom analizom nalazi se na sljedećoj poveznici: http://ubnixmalwareanalysis.blogspot.com/ Sljedeći korak je probati analizirati neki zapakirani malware te proučiti najpoznatije packere/unpackere. U tu svrhu ću također napisati blog kada završim.