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. tjedan (4.11 - 10.11.2013.)

Dosadašnji rad

Daljnji koraci

---

4. tjedan (11.11 - 17.11.2013.)

Dosadašnji rad

---

5. tjedan (18.11 - 24.11.2013.)

Dosadašnji rad