Test final de laborator - POO 2021
Data 29.05.2021
Timp: 120 minute
Timp predare pe email + incarcare Moodle: 5 minute (12:00 - 12:05)

Enunț:

Firma SmallCompany a fost victima unor atacatori cibernetici și un număr mare de calculatoare din cadrul companiei a fost compromis cu diverse tipuri de malware. Analistul de securitate a reușit să identifice clasele generale de malware de pe dispozitive și să extragă anumite informații despre acestea. Folosind aceste informații dorește să obțină ordinea dispozitivelor infectate în funcție de impact pentru a ști care este prioritatea acestora pentru carantinare. Informațiile strânse le are trecute pe o hârtie și colaborează cu studenții de la Facultatea de Matematică și Informatică în ideea dezvoltării unei aplicații care permite automatizarea procesului de ordonare a dispozitivelor.

Tipurile de malware ce se regăsesc sunt: Rootkit, Keylogger, Kernel-Keylogger și Ransomware.

Este nevoie de o aplicație ce permite actualizare în cazul apariției unor alte clase de malware.

Prin malware înțelegem un software rău intenționat pentru care se reține ratingul impactului (număr real), data de infectare (zi, luna, an), numele acestuia (care poate să fie format din mai multe cuvinte), metoda de infectare (dacă se cunoaște, altfel se reține șirul “unknown”) și un vector cu registrii modificați (reținuți ca stringuri).

Prin rootkit înțelegem un tip de malware ce are drept scop obținerea drepturilor de administrator asupra dispozitivului infectat. Pentru rootkit se reține lista importurilor care poate fi unul și oricât de multe (importurile fac referire la numele fișierelor .dll folosite) și o listă de stringuri semnificative (anumite stringuri dintr-un binar pot fi un indice asupra faptului că fișierul este rău intenționat).

Prin keylogger înțelegem un malware care înregistrează acțiunile de la tastatură și le trimite mai departe. Pentru un keylogger se reține o listă cu funcțiile folosite și o listă cu tastele speciale definite.

Prin kernel-keylogger înțelegem un keylogger ce rulează în kernel-mode (de obicei prin intermediul unui rootkit). Prin urmare, putem considera că este are atât proprietățile unui rootkit cât și ale unui keylogger. În plus, dorim să memorăm dacă ascunde fișiere și registrii.

Prin ransomware înțelegem un malware care criptează fișiere de pe disk. Pentru acesta se reține ratingul de criptare (un număr de la 1 la 10) și un rating de obfuscare (un număr real ce reprezintă procentul de obfuscare (obfuscare = metodă de a ascunde/îngreuna intenția inițială a codului)).

Pentru fiecare computer din firmă se reține un id unic, incrementat automat, o listă de malware (poate conține un malware sau mai multe) și ratingul final ce este calculat drept suma ratingului impactului fiecărui malware.

Modalitatea de calculare a ratingului impactului pentru fiecare clasa de malware:

Pentru fiecare malware ratingul impactului pornește de la 0.

Pentru rootkit ratingul impactului crește cu 100 dacă se întâlnește unul din stringurile “System Service Descriptor Table”, “SSDT”, “NtCreateFile”. Dacă se regăsește importul “ntoskrnl.exe”, valoarea impactului se dublează (importurile se verifică după stringuri).

Pentru keylogger ratingul impactului crește cu 10 la întâlnirea stringurilor “[Up]”, “[Num Lock]”, “[Down]”, “[Right]”, “[UP]”, “[Left]”, “[PageDown]” și cu 30 la întâlnirea unei din funcțiile: “CreateFileW”, “OpenProcess”, “ReadFile”, “WriteFile”, “RegisterHotKey”, “SetWindowsHookEx”.

Pentru kernel keylogger se respectă valorile de la rootkit și keylogger și se adaugă valoarea 20 dacă ascunde fișiere, respectiv valoarea 30 dacă ascunde registrii.

Pentru ransomware se adună ratingul de criptare cu ratingul de obfuscare.

Pentru orice tip de malware se adună 20 dacă registrii afectați sunt “HKLM-run” sau “HKCU-run”.

Programul realizat trebuie să aibă un meniu care permite:

1. afișarea informațiilor pentru fiecare calculator
2. afișarea informațiilor pentru fiecare calculator fiind ordonate după ratingul final
3. afișarea primelor k calculatoare ordonate după ratingul final
4. afișarea procentului de computere infectate din firmă

Să se folosească cât mai multe concepte de programare orientată pe obiecte din ceea ce s-a studiat la curs, seminar și laborator.

Mențiuni:

- Pentru nota 5 este necesară memorarea, citirea și afișarea a **n** calculatoare și pentru fiecare calculator să fie permisă memorarea, citirea și afișarea a **m** tipuri de malware. (FĂRĂ A FI NECESARĂ CALCULAREA RATINGULUI PENTRU MALWARE / CALCULATOR)
- Trebuie să fie folosite CÂT MAI MULTE concepte de POO pentru o notă cât mai mare
- Nota maximă este 12
- Nu aveți voie cu date PUBLIC (=> nota 1)
- Trebuie să aveți cameră WEB și microfon
- Aveți nevoie de legitimație pentru identificare/sau o poza cu legitimația/orice act de identitate.
- Nu se punctează codul comentat
- Programul trebuie sa ruleze.
- Subiectele se trimit în intervalul orar 12:00-12:05
- (moodle UB sau examen.oop.fmi@gmail.com de pe adresa instituțională)
- Nume folder / fișier: Grupa_NUME_PRENUME
- Depunctăm folosirea excesivă a implementării funcțiilor inline în clase.

MULT SUCCES!