Intrument pentru analiza securității rețelelor de comunicații

Rezumat

Student: Cosmin Dorcu

Grupa: 1404A

Specializare: C

Coordonator: Conf. Dr. Ing. Mihai Zaharia

Rezumatul lucrării

Această lucrare își propune să abordeze implementarea unei aplicații de analizare a securității rețelelor prin tehnici de scanare. Aceasta scanare presupune căutarea activă a tuturor dispozitivelor active pe rețea și culegerea unor informații despre acesta cum ar fi: adresa fizică (MAC), adresa IP, tipul de sistem de operare rulat și porturile TCP si UDP accesibile prin rețea. Pentru a obține aceste informații, aplicația implementează un număr de tipuri de scanări predefinite, dar și permite utilizatorilor definirea propriilor metode de scanare.

Deși această aplicație ar putea fi folosită în hacking, deoarece permite oricărui utilizator de pe o rețea să culeagă informații despre restul utilizatorilor (iar aceste informații pot fi folosite ulterior în atacuri), „Network Analysis" e destinat administratorilor de rețea, care pot astfel identifica mai uşor posibilele vulnerabilități ale rețelei.

Descrierea implementării

Aplicația are următoarele caracteristici:

- Modulul de bază este implementat in C++.
- Este disponibilă pe Windows și Linux.
- Are atât o interfață consola (Windows și Linux), cât și o interfață grafică (Windows).
- Interfața grafică este implementată in C# folosind VPF. Accesarea funcționalităților implementate nativ este folosit un wrapper C++/CLI.

Dependințe:

- Boost 1.59 – bibliotecă generală C/C++ cross-platform, aleasă pentru a simplifica anumite implementări (de exemplu parsarea liniei de comandă), cât și pentru portabilitatea ei. Este inclusă în proiect în varianta unei biblioteci statice.
- WinPCap 4.1.3 – bibliotecă de networking C/C++ cross-platform. Este folosită pentru manipularea socket-urilor la nivel low, ceea ce permite scrierea pachetelor de date de la 0, după necesitate. Este inclusă în forma unui *.lib*, însă pentru accesarea socket-urilor raw este necesar un driver ce trebuie instalat separat de aplicație.

Structura proiectului:

- Windows
  - Mediul de dezvoltare folosit este Visual Studio 2013
  - Soluția cuprinde proiectele:
    - Netscan – dll C++ – modulul principal unde sunt implementate toate operațiile cu rețeaua și analizarea datelor. Expune o interfață ce e apelată de celelalte proiecte

- NetAnalysis – exe C++ – interfața consolă, permite accesarea tuturor operațiilor implementate in modulul dll
- Netscan_wrapper – dll C++/CLI – dll ce expune aceleași metode expuse si de modulul 'netscan' și e accesibil din aplicația managed
- NetAnalysisGUI – exe C# - interfața grafică a aplicației. Conține toate functionalitățile aplicației consolă.

- Linux (build făcut pe Ubuntu)
  - Mediul de dezvoltare: Eclipse Luna
  - Un singur proiect conține build-ul la aceleași fișiere sursă conținute în proiectele „Netscan" și „NetAnalysis", rezultatul fiind un executabil echivalent ca funcționalitate cu „NetAnalysis".

Functionalități implementate:

- Discovery scan – pentru fiecare adresă din mulțimea specificată la intrare este trimis un pachet ARP. Dacă la o adresă este activă o stație, aceasta va răspunde cu un alt pachet ARP. În acest moment aplicația preia adresa IP și MAC a țintei, împreună cu timpul de răspuns.
- TCP Syn Scan – metoda cea mai folosită în maparea porturilor TCP deschise și închise ale unei stații. Pentru fiecare stație și pentru fiecare port specificat, aplicația construiește un pachet TCP de tip SYN și îl trimite țintei. Ținta poate răspunde cu:
  - Un pachet TCP SYN/ACK, care marchează faptul că acel port este deschis și acceptă conexiuni
  - Un pachet TCP RST, portul fiind marcat ca accesibil dar nicio aplicație nu ascultă acel port
  - Niciun răspuns sau un pachet ICMP (tip 3 - unreachable error, cod 0, 1, 2, 3, 9 sau 13), ceea ce marchează portul ca filtrat, adică starea lui nu poate fi determinată, accesul fiind blocat (de exemplu de un firewall). Această este stabilită după un număr de încercări (setabil de către utilizator), ceea ce încetinește scanarea considerabil
- TCP Fin/Null/Xmass scan – trei tipuri de scanare similare care pot evita anumite IDS-uri, în schimb nu returnează la fel de multe informații ca un Syn Scan. Este trimis un pachet TCP cu flag-urile setate în funcție de tipul de scanare selectată. Dacă primește ca răspuns un pachet TCP RST, portul este marcat ca închis. Dacă, după un număr de încercări, nu se primește niciun răspuns, portul e marcat ca filtrat|deschis. Dacă un pachet ICMP este primit, portul e marcat ca filtrat.
- TCP Custom Scan: permite user-ului constuirea flag-urilor TCP și setarea interpretării tipului de răspuns: ca pe un răspuns al unei scanări SYN, sau un răspuns ca al unei scanări FIN.

Pe lângă acestor scanări implementate, în interfața grafică utilizatorul poate construi pachete de la zero, ceea ce poate fi util atât în testarea rețelei și detectarea vulnerabilităților, cât și în testarea aplicațiilor ce rulează pe stațiile de pe rețea.