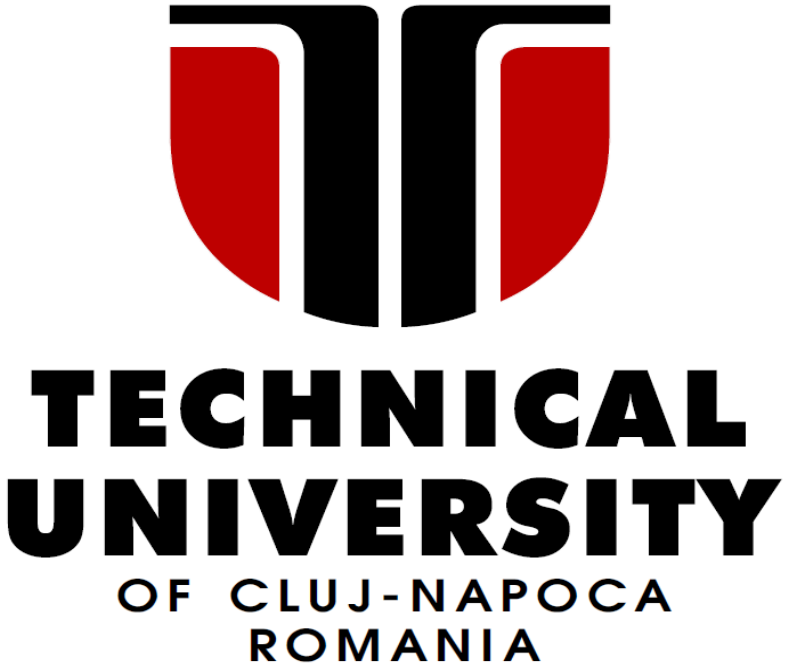

Proiect ASO 2024: Management-ul unui botnet

Documentatie - Etapa 3

Iamnitchi Bogdan - Grupa 30461

Administrarea Sistemelor de Operare
Facultatea de Automatica si Calculatoare
2024-2025

Cerinte rezolvate

Am dezvoltat un script Python pentru detectarea atacurilor brute force generate de malware-ul Mirai, concentrându-mă pe identificarea mai multor tipuri de atacuri. Soluția implementează algoritmi avansați de analiză a pachetelor, folosind biblioteca **Pyshark**, și detectează următoarele tipuri de atacuri:

1. **SYN Flood**
    - Detectează un volum ridicat de pachete SYN care nu finalizează handshake-ul TCP, ceea ce indică un atac de tip DoS.
    - Monitorizează timpul de sosire și numărul conexiunilor SYN pe un anumit port al serverului pentru a determina activitatea suspectă.
2. **ACK Flood**
    - Identifică fluxuri de pachete ACK trimise fără o conexiune preexistentă, forțând serverul să răspundă cu pachete RST.
    - Analizează flag-urile TCP și numărul de pachete într-un interval scurt de timp.
3. **UDP Flood**
    - Detectează un număr mare de pachete UDP trimise către un port țintă de pe porturi multiple, simulând un atac de saturație.
    - Include verificări suplimentare pentru a analiza consistența dimensiunii pachetelor trimise.
4. **UDP Plain Flood**
    - Similar cu UDP Flood, dar cu accent pe detectarea atacurilor care utilizează pachete UDP de dimensiuni fixe și date repetate, un semn distinctiv al atacurilor Mirai.
5. **GRE IP Flood**
    - Monitorizează pachetele GRE (Generic Routing Encapsulation) și identifică fluxuri care saturează serverul țintă.

Implementare Tehnică

Am dezvoltat clase dedicate pentru fiecare tip de atac, cu funcții care:

- Captură și analizează traficul în timp real.
- Utilizează reguli personalizate pentru fiecare tip de atac, bazate pe numărul de pachete, timpii de sosire și pattern-uri detectate în payload.
- Raportează evenimentele suspecte, oferind informații detaliate despre sursa, destinația și porturile implicate.

Acest script reprezintă o soluție scalabilă și eficientă pentru monitorizarea traficului de rețea și detectarea atacurilor Mirai.

Probleme întâlnite și modul de rezolvare

Să fiu sincer, lucrul la scriptul pentru detectarea atacurilor Mirai a fost o provocare interesantă. Am început cu ideea că folosind Pyshark ar trebui să fie destul de simplu să analizez pachetele, dar realitatea a fost mai complicată. Una dintre primele întrebări pe care mi le-am pus a fost cum să identific în mod clar diferitele tipuri de atacuri (SYN flood, ACK flood, UDP flood) din fluxul continuu de trafic. Mi-am dat seama rapid că trebuie să definesc clar semnăturile pentru fiecare tip de atac și să decid ce înseamnă "suspect" în termeni de număr de pachete și intervale de timp.

O altă problemă a fost să fac diferența între traficul normal și traficul de atac. Spre exemplu, pentru SYN flood, aveam nevoie să identific rapid pachetele care inițiau conexiuni, dar fără să fie urmate de răspunsuri normale. Am petrecut destul timp ajustând valorile pentru numărul de pachete și intervalele în care consider un atac. Am avut momente în care mă întrebam dacă detectez cu adevărat atacuri sau doar false pozitive din cauza traficului normal din rețea.

La partea cu UDP flood, lucrurile au fost și mai complicate. Mirai folosește pachete cu o lungime fixă, dar asta nu înseamnă că fiecare flux cu pachete de aceeași lungime e un atac. A trebuit să implementez verificări suplimentare, cum ar fi analiza porturilor folosite și frecvența pachetelor, ca să fiu sigur că detectez corect. Chiar și așa, la început am avut rezultate mixte și m-am întrebat dacă logica mea e prea simplistă sau dacă ar trebui să introduc un filtru mai avansat.

La partea de GRE IP, lucrurile au fost mai confuze pentru că nu eram sigur cum să extrag informația relevantă din pachete. A trebuit să înțeleg formatul pachetelor GRE și să văd cum să le identific corect. Nu m-aș fi gândit înainte cât de mult timp poate să îți ia să înveți doar să parcurgi structura unui pachet și să extragi flagurile sau informațiile care contează.