Analýza botnetov pomocou honeypotov

Mgr. Tomáš Bajtoš vedúci práce: RNDr. JUDr. Pavol Sokol PhD.

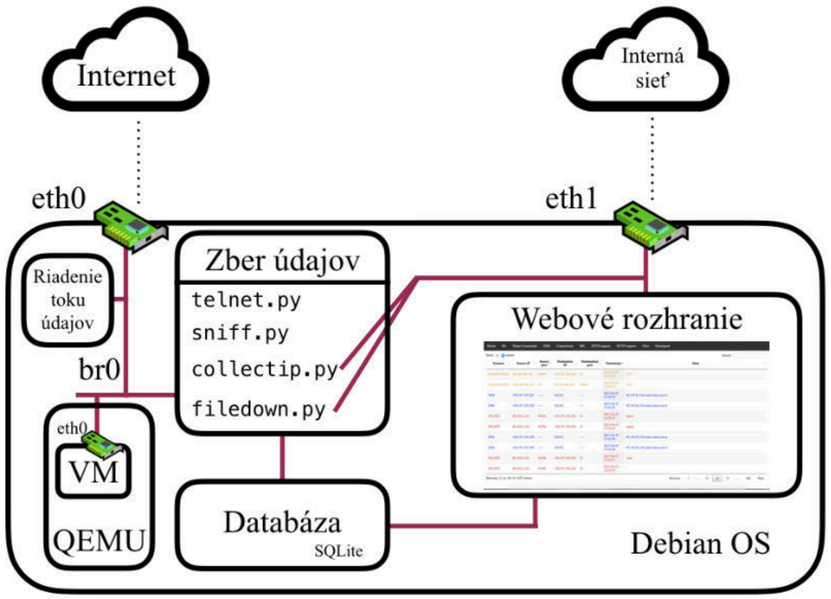
ÚSTAV INFORMATIKY, PRÍRODOVEDECKÁ FAKULTA, UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Motivácia

- Botnety sú vážnou hrozbou pre informatickú bezpečnosť.
- Rastie počet útokov a aj sila, akou botnety útočia na svoj cieľ.
- Množstvo botnetov využíva na šírenie nezabezpečenú telnet komunikáciu.
- Zneužitie slabo zabezpečených zariadení, akými sú napríklad domáce smerovače, sa ukazuje ako vhodný spôsob fungovania botnetu. Takéto zariadenia sú postavené na rôznych architektúrach.
- Honeypoty umožňujú sledovať aktivitu botnetu už od počiatočného štádia šírenia.

Implementácia

- Navrhli a implementovali sme vysoko interaktívny honeynet.
- Celý honeynet je pripojený k univerzitnej sieti a jeho činnosť je zaznamenávaná.
- Zaznamenávame všetku TCP a UDP komunikáciu.
- Zvlášť sa zameriavame na telnet komunikáciu. Uchovávame konkrétne príkazy použité pri útoku.
- Virtuálne honeypoty sú postavené na rôznych architektúrach procesorov.
- Pri nakazení honeypotu máme možnosť stiahnuť škodlivý kód.
- Zozbierané údaje je možné zobraziť vo webovom rozhraní, čo umožňuje ich ľahšie skúmanie.



Výsledky

- Nami navrhnutý honeynet už počas prvých minút svojho fungovania zaznamenal činnosť botnetu Mirai a iných botnetov.
- Potvrdil schopnosť vysoko interaktívnych honeypotov zaznamenať činnosť rôznych botnetov využívajúcich nezabezpečenej služby telnet.
- Zozbieral binárne súbory použité pri šírení botnetov.
- Poukázal na potrebu lepšieho zabezpečenia zariadení využivajúcich službu telnet.
- Potvrdil hypotézu, že pri šírení botnetu zohráva úlohu aj architektúra procesora zariadenia.
- Za pomoci honeynetu sme zaznamenali jednotlivé kroky útočníka pri pokuse nakaziť zariadenie škodlivým kódom.