Rozšírené zadanie diplomovej práce

Názov práce: Detekcia prvotných fáz kybernetických útokov
Autor: Bc. Martina Pivarníková
Vedúci práce: JUDr. RNDr. Pavol Sokol, PhD.
Konzultant: Mgr. Tomáš Bajtoš
Školiace pracovisko: ÚINF - Ústav informatiky

Ciele:

1. Analýza, porovnanie a spracovanie aktuálnych prístupov k modelovaniu kybernetických útokov
2. Vytvorenie modelovej dátovej sady z bezpečnostných udalostí
3. Návrh, implementácia a vyhodnotenie modelu na detekciu prvotných fázach kybernetických útokov

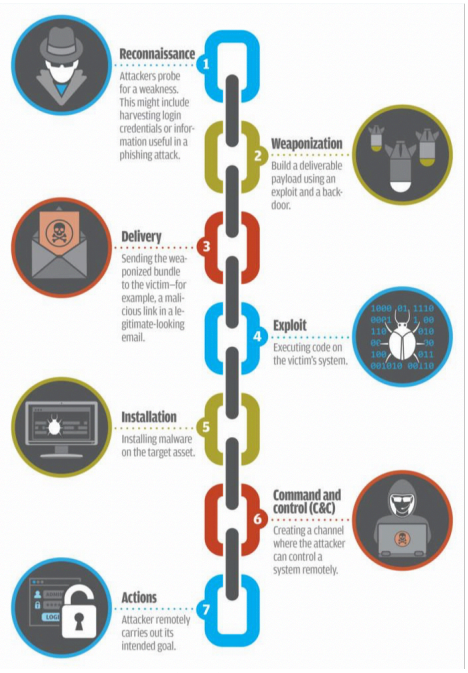
Popis:

V dnešnej dobe čelíme mnohým kybernetickým hrozbám. Z tohto dôvodu je potrebné neustále vyvíjať rôzne riešenia na obranu. Každý deň dôjde na celom svete k veľkému počtu útokov. Dokážeme sa z nich poučiť a využiť tieto znalosti na vytvorenie nástrojov na ochranu pred útokmi a na ich predikciu.

Okrem vyvíjania prevenčných systémov je potrebné sústrediť sa rovnako aj na detekčné systémy, ktoré nám pomôžu získať informácie o hrozbách a útokoch. Tieto údaje dokážeme využiť na neustále zlepšovanie daných systémov tak, aby dokázali detegovať každú fázu útoku. Takto budeme vedieť odhaliť skoršie fázy útoku a predikovať, ako budú postupovať. Týmto spôsobom je možné sa efektívnejšie brániť proti známym typom útokov.

V prvej časti tejto práce sa budeme venovať analýze aktuálnych prístupov k modelovaniu bezpečnostných udalostí. Na základe vykonanej analýzy si zvolíme najvhodnejšie spôsoby na modelovanie, ktoré budeme využívať. V tejto práci sa však budeme prevažne venovať modelovaniu kybernetických útokov pomocou „Cyber kill chain“ modelu jeho modifikácií. Tento model nám umožňuje identifikovať rôzne štádiá útoku. Jeho schému môžeme vidieť na Obrázku č.1.

Vďaka identifikácii viacerých kill chainov môžeme identifikovať spoločné a prekrývajúce sa ukazovatele. Takáto analýza je nápomocná k určovaniu taktík, techník a postupov útočníkov. Taktiež je veľmi dôležité zistiť zámer útočníka a identifikácia kill chainu nám k tomu môže dopomôcť. Pomocou identifikácie útoku v jeho skorších fázach vieme predikovať, ako bude útok pokračovať. Na základe toho je možné v rámci organizácie zaviesť preventívne opatrenia.



Obr. 1 Cyber kill chain [1]

Druhým krokom diplomovej práce bude vytvorenie modelovej dátovej sady z bezpečnostných udalostí získaných z Wardenu a honeynetu. Honeynet predstavuje sieť honeypotov, teda pascí na útočníkov. V každej takejto udalosti budú identifikované fázy útoku. Týmto dokážeme vytvoriť databázu útokov, ktorá bude základom pre návrh modelu a samotnú implementáciu systému na predikciu etáp v rámci útokov.

Podstatou navrhnutého systému by mala byť identifikácia kybernetického útoku v jeho skorších fázach. Tento systém by mal dokázať predpokladať ďalšie kroky identifikovaného útoku. Predikcia bude založená na modelových dátach a porovnávaní ich signatúr so zachyteným útokom. Na záver tento systém zavedieme do prevádzky a vyhodnotíme jeho úspešnosť v rámci detekcie.

[1] https://www.csoonline.com/article/2134037/

Literatúra:

[1] SHOSTACK, Adam. Threat modeling: Designing for security. John Wiley & Sons, 2014.

[2] UCEDAVELEZ, Tony; MORANA, Marco M. Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. John Wiley & Sons, 2015.

[3] YAN, Xiaohua; ZHANG, Joy Ying. Early detection of cyber security threats using structured behavior modeling. ACM Transactions on Information and System Security, 2013.

[4] ERTAUL, Levent; MOUSA, Mina. Applying the Kill Chain and Diamond Models to Microsoft Advanced Threat Analytics. 2018

[5] HUTCHINS, Eric M.; CLOPPERT, Michael J.; AMIN, Rohan M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 2011, 1.1: 80.