Identifikácia fáz útoku v počítačovej sieti

Diplomová práca – rozšírené zadanie

Vedúci práce: doc. RNDr. JUDr. Pavol Sokol, PhD.

Konzultant: RNDr. Tomáš Bajtoš

Úvod

Kybernetické útoky ohrozujú používateľov a organizácie už od vzniku internetu. Spolu s počítačovými sieťami sa však stali oveľa viac zložitejšími. V dnešnej dobe potrebujú útočníci vykonať aj niekoľko krokov, aby dosiahli svoj konečný cieľ. Množinu takýchto krokov označujeme ako viacstupňový útok alebo scenár útoku. Ich viacstupňový charakter bráni detekcii narušenia systému, keďže na pochopenie stratégie útoku a identifikáciu hrozby je potrebná korelácia viac ako jednej akcie. Od začiatku roku 2000 sa komunita výskumníkov v oblasti bezpečnosti pokúsila navrhnúť riešenie na detekciu tohto druhu hrozby a predikovať ďalšie kroky útoku.

Pokročilí útočníci postupujú krok za krokom pri ich pokusoch o vykonanie útoku na systém. Je to hlavne z dôvodu, že obete zvolené útočníkmi sú zvyčajne stredné alebo veľké organizácie so zložitou topológiou siete a rôznymi vrstvami zabezpečenia. Vzhľadom na to, že najdôležitejšie dáta z hľadiska hodnoty informácie sú umiestnené v menej dostupných častiach siete, bolo by viac-menej nemožné uskutočniť úspešný prienik do systému pomocou jednokrokového útoku. Ďalším dôvodom je to, že ak sa útok rozloží na niekoľko krokov, tak je nenápadnejší a ťažšie identifikovateľný obeťou, najmä ak niektoré z krokov sami o sebe nepredstavujú riziko pre systém.

V tejto práci budeme pracovať s datasetom. Dataset predstavuje reálne dáta zo stredne veľkej organizácie, na ktorú bol odsimulovaný viacstupňový útok. Dáta sú z koncových staníc, emailového servera, webového servera a ďalších zdrojov.

Cieľom práce je na týchto dátach detegovať odsimulovaný viacstupňový útok a identifikovať jeho fázy/kroky v čase. Zároveň by sme takto chceli zistiť, akú taktiku a techniky spadajúce pod túto taktiku, útočník využil.

Našimi najbližšími krokmi bude dôkladnejšie oboznámenie sa s datasetom a následný návrh vhodného modelu na identifikáciu fáz útoku, čo si samozrejme bude vyžadovať preštudovanie podobných prác, v ktorých sa autori venovali takejto problematike.

Ciele práce

1. Analyzovať prístupy k identifikácii fáz útoku v počítačovej sieti.
2. Porovnať prístupy k identifikácii fáz útoku v počítačovej sieti pomocou digitálnych stôp z koncových zariadení.
3. Navrhnúť a implementovať model identifikácie fáz útoku v počítačovej sieti, vyhodnotenie efektívnosti tohto modelu.

Literatúra

1. Navarro, J., Deruyver, A., & Parrend, P. (2018). A systematic survey on multi-step attack detection. Computers & Security, 76, 214-249.
2. Aparicio-Navarro, F. J., Kyriakopoulos, K. G., Ghafir, I., Lambotharan, S., & Chambers, J. A. (2018, October). Multi-stage attack detection using contextual information. In MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM) (pp. 1-9). IEEE.
3. Takey, Y. S., Tatikayala, S. G., Samavedam, S. S., Eswari, P. L., & Patil, M. U. (2021, March). Real Time early Multi Stage Attack Detection. In 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 283-290). IEEE.
4. Wilkens, F., Ortmann, F., Haas, S., Vallentin, M., & Fischer, M. (2021, November). Multi-Stage Attack Detection via Kill Chain State Machines. In Proceedings of the 3rd Workshop on Cyber-Security Arms Race (pp. 13-24).