Rozšírené zadanie diplomovej práce

Názov: Grafy útokov v kybernetickej bezpečnosti

Autor: Bc. Vladimír Homola

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

Konzultant: MSc. Terézia Mézešová

Ciele práce:

1. Preskúmať možnosti použitia grafov útokov s prihliadnutím na aktuálne bezpečnostné hrozby
2. Analyzovať a porovnať prístupy ku generovaniu a vizualizácii grafov útokov v kybernetickej bezpečnosti
3. Navrhnúť a implementovať systém na generovanie a vizualizáciu grafov útokov v kybernetickej bezpečnosti

Počítačové siete zohrávajú dôležitú úlohu v našom každodennom živote. Denne nimi prejde obrovské množstvo dát. Preto je dôležité vedieť, aké dáta počítačovou sieťou prechádzajú, či už z hľadiska administrácie siete, stability alebo bezpečnosti.

V dnešnej dobe sa kybernetické útoky dejú dlhodobo a systematicky, na rozdiel od minulosti, kedy boli organizované skôr jednoducho a zväčša náhodne. Informačná a kybernetická bezpečnosť sa stáva viac a viac dôležitou a organizácie, resp. štátne organizácie investujú nemalé peniaze na ochranu svojej kritickej infraštruktúry. Súčasne samotné kybernetické útoky sú čím ďalej, tým viac komplexné, premyslené a s ničivými dôsledkami.

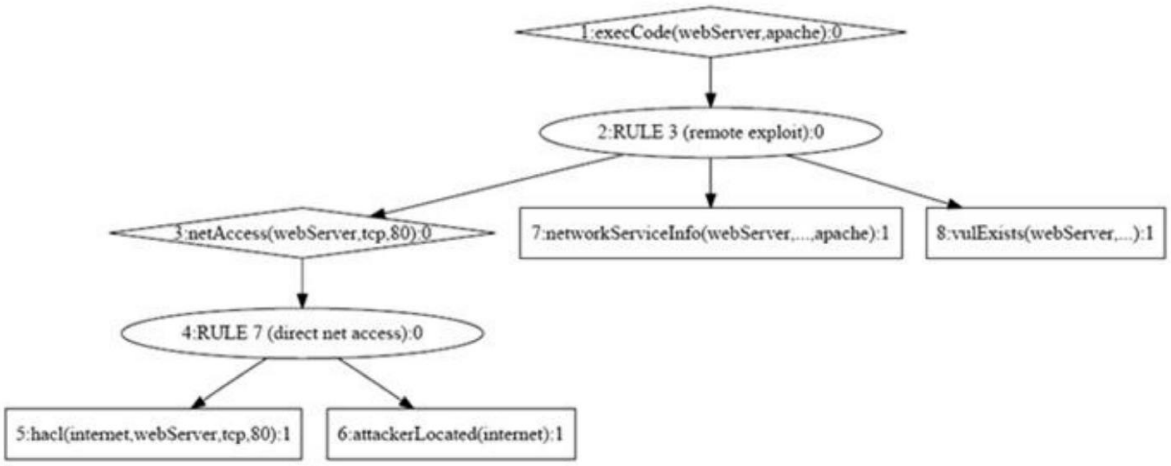
Vnímanie a pochopenie kybernetických útokov môže byť náročná úloha. Na pomoc pri vnímaní kybernetických útokov sú potrebné účinnejšie techniky. Techniky modelovania útokov, tzv. AMT (Attack modelling techniques), ako sú grafy útokov, stromy útokov a stromy porúch, sú populárne metódy matematického a vizuálneho znázornenia sledu udalostí, ktoré

môžu viesť k úspešnému kybernetickému útoku. Práve tieto metódy vedia byť užitočnými vizuálnymi pomôckami, ktoré môžu pomôcť pri vnímaní kybernetických útokov.

Graf útokov vie simulovať možné cesty, akými by vedel potencionálny útočník napadnúť danú počítačovú sieť organizácie. Pomocou grafu útokov vie administrátor siete vyhodnotiť bezpečnosť siete a analyzovať a predpovedať správanie útočníka.

Hovorí sa, že reťaz je len tak pevná, ako je pevný jej najslabší článok. Toto isté sa dá povedať o bezpečnosti počítačovej siete. Môžeme mať dobre zabezpečenú sieť, ak sa však v nej nájde nejaká slabina, tak hacker využije práve ňu počas útoku. Slabiny nemusia byť vždy navonok viditeľné a na ich detekciu je treba podrobnejšie analyzovať danú sieť (poznať topológiu danej siete). Toto sa dá robiť manuálne alebo automatizovane použitím nejakého z nástrojov na generovanie topológie siete, správu zraniteľností.

Cieľom diplomovej práce je vytvorenie nástroja, ktorý bude vedieť na základe topológie, nastavenia siete, zoznamu zraniteľností, predpokladov a cieľov útoku vygenerovať graf potencionálneho útoku ako napríklad na Obr. 1. Budeme sa inšpirovať open-source softvérom MulVAL [4], čiže jedným z prvých krokov okrem naštudovania si potrebnej literatúry bude analyzovať, ako tento softvér funguje a jeho zdrojové kódy. Následne na základe zistených poznatkov navrhneme a implementujeme vlastný softvér. Tu bude veľa priestoru na experimentovanie s tým, ako pracovať so vstupnými dátami a ako ich vizualizovať, čo bude tvoriť vrcholy a hrany grafu-prípadne dať možnosť administrátorovi nastavovať rôzne parametre podľa potreby a na základe toho prekreslovať graf, čo by bolo záverom našej práce.



Obr. 1 MulVAL: graf ciest útoku [6]

Literatúra:

1. ZENG, Jianping, et al.: Survey of attack graph analysis methods from the perspective of data and knowledge processing. Security and Communication Networks, 2019.

2. WANG, Lingyu; JAJODIA, Sushil; SINGHAL, Anoop. Network Security Metrics. Springer, 2017.

3. KAYNAR, Kerem. A taxonomy for attack graph generation and usage in network security. Journal of Information Security and Applications, 2016, 29: 27-56.

4. OU, Xinming; GOVINDAVAJHALA, Sudhakar; APPEL, Andrew W. MulVAL: A Logic-based Network Security Analyzer. In: USENIX Security Symposium. 2005. p. 8-8.

5. LALLIE, Harjinder Singh; DEBATTISTA, Kurt; BAL, Jay. A review of attack graph and attack tree visual syntax in cyber security. *Computer Science Review*, 2020, 35: 100219.

Zdroje:

6. https://cordis.europa.eu/docs/projects/cnect/8/285248/080/deliverables/001-D841bFIWAREUserandProgrammersGuide.pdf

Pavol Sokol
2021.12.01
16:27:21
+01'00'