ROZŠÍRENÉ ZADANIE DIPLOMOVEJ PRÁCE

Názov práce: Grafy útokov v kybernetickej bezpečnosti

Autor: Bc. Šimon Javorský

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

Konzultant: Mgr. Terézia Mezešová

Školiace stredisko: ÚINF – Ústav informatiky

Ciele:

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.

Popis:

Reťaz je len tak pevná, ako jej najslabší článok. To isté platí aj o bezpečnosti v počítačovej sieti. Všetky uzly môžu byť dôkladne zabezpečené, ale ak existuje cesta, ktorou sa hacker ľahko dostane k svojmu cieľu, je námaha vynaložená na zabezpečenie siete úplne zbytočná.

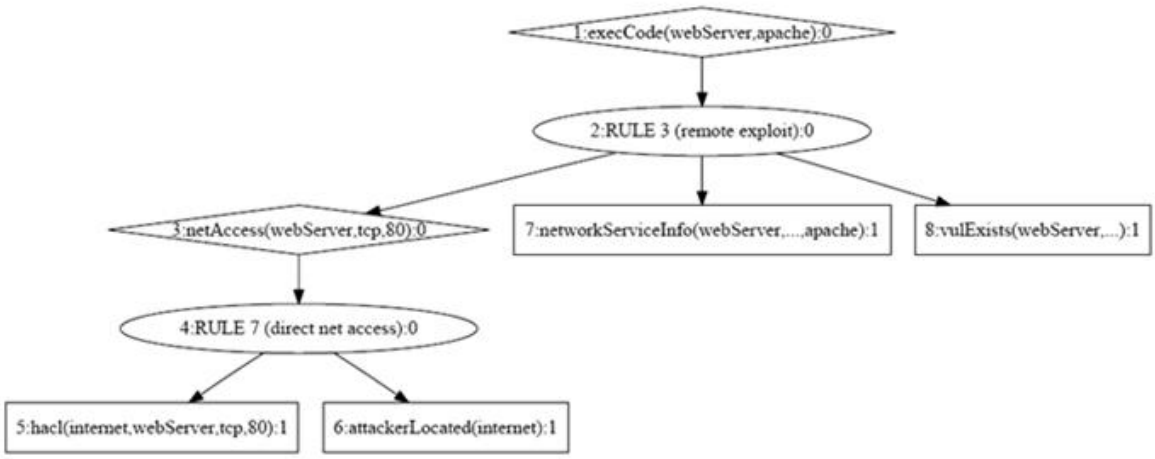
Na zistenie takejto slabiny je nutné poznať topológiu celej siete a konfiguráciu jednotlivých počítačov a routrov. Tieto informácie je možné zozbierať manuálne, čo je však pri sieťach veľkých rozmerov takmer nemožné. Existujú na to teda automatizované riešenia, pričom jedným z nich je *OpenVAS*, ktorý budeme používať. OpenVAS je framework pozostávajúci z viacerých nástrojov a služieb, ponúkajúci komplexné riešenia pre skenovanie a správu zraniteľností.

Ďalším faktorom ovplyvňujúcim zabezpečenie počítačovej siete je znalosť aktuálnych zraniteľností. Iné bezpečnostné hrozby sa riešili pred desiatimi rokmi a iné sa riešia teraz. Pre riešenie tohto problému použijeme repozitár štandardizovaných zraniteľností *National Vulnerability Database* (NVD) od *National Institute of Standards and Technology*. Tieto dáta nám umožňujú automatizáciu spravovania bezpečnostných hrozieb.

Keď máme k dispozícii konfiguráciu siete, zoznam zraniteľností, ktoré sa v nej môžu vyskytovať, vieme si predstaviť motív a cieľ útoku, čo môže byť odstavenie konkrétnej služby, či získanie, prípadne odstránenie citlivých dát, je potrebné ešte doplniť predpoklady útoku. K nim patrí napr. informácia, ktoré počítače a routre sú verejne prístupné, ktoré sú pripojené k internetu a podobne.

Následne môžeme použiť softvér, ktorý tieto dáta vyhodnotí a vygeneruje najzraniteľnejšiu cestu v rámci našej počítačovej siete. Väčšinou však ide o drahé aplikácie, prípadne je táto služba

súčasťou drahého komplexného balíka pre správu sietí. Asi jediným použiteľným open-source riešením tohto problému sa ponúka *MulVAL*. MulVAL je výskumný nástroj pre bezpečnostných technikov a správcov systémov, pomáha riadiť konfiguráciu veľkých sietí a kontrolovať bezpečnostné hrozby. Je to ale starší projekt, čo vytvára viacero problémov s kompatibilitou. Napríklad v rámci NVD nepodporuje zraniteľnosti verzie V3, ktoré poskytujú lepšie informácie a presnejšie zaradenie v hodnotení závažnosti.



Obrázok 1 *MulVAL: malý graf ciest útoku*

Cieľom tejto diplomovej práce je vytvoriť nástroj, ktorý bude vedieť na základe konfigurácie siete, zoznamu aktuálnych zraniteľností, predpokladov a cieľov útoku vygenerovať graf takéhoto útoku. Dôraz sa pritom kladie na kompatibilitu s aktuálnymi technológiami. V tejto práci sa budeme inšpirovať predovšetkým MulVALom. Keďže je to open-source softvér, prvým krokom bude analyzovať spôsob fungovania a zdrojové kódy tohto programu. Ďalšími krokmi bude návrh a implementácia vlastného softvéru. Tu sa budú riešiť aj otázky akým spôsobom predspracovávať vstupné dáta, v akom formáte ukladať vygenerované grafy, ako ich vizualizovať a ako s nimi ďalej pracovať. Na záver je ešte priestor pre riešenie dynamickej práce s grafom, kde si užívateľ môže zobraziť, ako by vyzeral graf bez jeho zvolených zraniteľností.

Literatúra:

1. WANG, Lingyu; JAJODIA, Sushil; SINGHAL, Anoop. Network Security Metrics. Springer, 2017.
2. KAYNAR, Kerem. A taxonomy for attack graph generation and usage in network security. Journal of Information Security and Applications, 2016, 29: 27-56.
3. OU, Xinming; GOVINDAVAJHALA, Sudhakar; APPEL, Andrew W. MulVAL: A Logic-based Network Security Analyzer. In: USENIX Security Symposium. 2005. p. 8-8.
4. SHEYNER, Oleg; HAINES, Joshua; JHA, Somesh; LIPPMANN, Richard; WING, Jeannette M. Automated Generation and Analysis of Attack Graphs. Berkeley, 2002.
5. OU, Xinming. A logic-programming approach to network security analysis. Princeton University, 2005.