Detekcia honeypotov

Autor: Bc. Lucia Kokuľová

Vedúci práce: JUDr. RNDr. Pavol Sokol, PhD.
Konzultant: Mgr. Tomáš Bajtoš

Ciele práce:

1. Analýza bezpečnosti honeypotov a vytvorenie odporúčaní pre tvorbu a používanie honeypotov z pohľadu nedetekovateľnosti
2. Porovnanie a vyhodnotenie existujúcich prístupov k detekcii honeypotov
3. Návrh, implementácia a vyhodnotenie nástroja/prostredia na detekciu honeypotov

V dnešnej dobe je takmer každé zariadenie v našich domácnostiach pripojené k internetu. Mnoho z týchto zariadení je nedostatočne zabezpečených a preto sa útočníkom každým dňom naskytá čoraz viac a viac šancí na to, aby tieto zariadenia napadli a využili vo svoj prospech. Na detekciu týchto útokov existujú rôzne nástroje. V rámci tejto záverečnej práce sa budeme venovať jednému z týchto nástrojov, konkrétne honeypotom.

Honeypot je bezpečnostný nástroj na detekciu a prípadné odvrátenie neautorizovanej manipulácie so systémom. Honeypot sleduje aktivitu útočníka v sieti, čím ho dokáže efektívne identifikovať a následne monitorovať jeho aktivitu. Jeho hodnota spočíva v tom, že ho útočník použije, honeypot by sa teda mal útočníkovi javiť ako dostupný cieľ. Jednou z najdôležitejších vlastností honeypotov je však skutočnosť, že útočník nemá vedomosť o tom, že sa pripája na honeypot (nedetekovateľnosť). Napriek tomu, že útočník má byť schopný neautorizovane použiť honeypot, nemôže byť schopný odhaliť to, že s ním komunikuje. V tomto prípade by hrozilo, že ukončí svoju aktivitu a tým by sa cieľ honeypotu – identifikácia útočníka, nepodarilo zrealizovať. Iným dôsledkom môže byť odlišné správanie útočníka.

Napriek skutočnosti, že nedetekovateľnosť je základná vlastnosť honeypotov, niektoré typy honeypotov je možné degekovať na základe ich charakteristických čŕt. Pri detekcii honeypotov je možné sledovať napríklad služby ponúkané sieťou, o ktorej chceme zistiť či je honeypotom. Môžeme sa pritom zamerať na to aké služby daná sieť ponúka a ktoré jej zas chýbajú. To nám môže napovedať viac o tom, či je sieť reálna alebo komunikujeme

s honeypotom. Inými vlastnosťami, ktoré pri detekcii môžeme využiť môže byť nezvyčajné správanie či používanie špecifických hardvérových zariadení. Metódou operačnej analýzy vieme monitorovať správanie systému, napríklad skúšaním rôznych funkcií a porovnávaním získaných výsledkov s očakávanými hodnotami.

Jedným z cieľov našej práce bude analyzovať bezpečnosť honeypotov a súčasne preskúmať možnosti používania honeypotov z pohľadu ich nedetekovateľnosti. Budeme sa teda zameriavať na vlastnosti honeypotov, ktoré by mohli túto vlastnosť narušiť a pokúsime sa nájsť spôsoby, ako by sa tomuto dalo zabrániť.

Detekcia honeypotov sa líši v závislosti od toho, aký typ honeypotu sa pokúšame detegovať. Pri identifikácii nízko-interaktívnych honeypotov (nízka interakcia spočíva v odpovediach na požiadavky útočníka) sa môžu využívať iné techniky ako pri identifikácii vysoko-interatívnych honeypotov (útočníkovi je poskytnutý reálny systém, resp. reálne prostredie). Detekcia pritom môže byť na úrovni počítačovej siete, aplikácií či systému. V našej práci sa budeme venovať aj aktuálnym prístupom, ktoré sú zamerané na detekciu honeypotov. Implementačným cieľom práce je návrh a implementácia nástroja, resp. prostredia na detekciu honeypotov. K tomuto účelu si vytvoríme honeynet obsahujúci najčastejšie používané typy honeypotov. Následne budeme tento nástroj, resp. prostredie vyhodnocovať. Vyhodnotenie bude spočívať v úspešnej detekcii honeypotov s prihliadnutím na false positive správy (označenie reálneho systému za honeypot).

Literatúra:

[1] NG, Chee Keong; PAN, Lei; XIANG, Yang. Honeypot Frameworks and Their Applications: A New Framework. Springer, 2018.

[2] UITTO, Joni, et al. A Surveyon Anti-honeypot and Anti-introspection Methods. In: World Conference on Information Systems and Technologies. Springer, Cham, 2017. p. 125-134.

[3] JOSHI, R. C.; SARDANA, Anjali. Honeypots: a new paradigm to information security. CRC Press, 2011.

[4] UITTO, Joni; RAUTI, S.; LAURÉN, S.; LEPPANÄN, V. A Survey on Anti-honeypot and Anti-introspection Methods. 2017.

[5] VETTERL, A; CLAYTON, R. Bitter Harvest: Systematically Fingerprinting Low- and Medium-interaction Honeypots at Internet Scale, 2018.