Posudek oponenta bakalářské práce

Student: Buchta David, Bc.
Téma: Nástroj na generování polymorfních síťových útoků (id 16688)
Oponent: Malinka Kamil, Mgr., Ph.D., UITS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

2. Splnění požadavků zadání **zadání splněno s drobnými výhradami**

Student splnil všechny body zadání. Výtku mám ke zpracování prvních tří bodů. V rámci seznámení se s problematikou útoků se student věnoval primárně obecným přístupům, v práci mi chybí důraz právě na polymorfní síťové útoky a útoky, které obsahují ve svém těle shellkód. Je jim věnován příliš malý prostor. Nejasnost mám i ohledně návrhu nástroje, který je velmi stručný, částečně převzatý a není jasné co je produktem studenta a co převzal.

3. Rozsah technické zprávy **je v obvyklém rozmezí**

Rozsah práce odpovídá BP. V přehledu současného stavu mi chybí větší sekce přehledu polymorfních útoku, dále chybí lepší přechod od obecného popisu ke specifickým částem relevantních k zadání BP. Zcela chybí diskuze k již existujícím nástrojům obdobného typu.

4. Prezentační úroveň předložené práce **65 b. (D)**

V práci jsou velké mezery, některé části jsou nelogicky členěny, např. zmínka o mutátorech, ačkoliv se jedná o významnou část řešení, se poprvé objevuje až v části návrhové, o jejich principu je jen velmi drobná zmínka v části implementace. Návrh aplikace je extrémně stručný, je inspirován již existujícím řešením, které není nikde popsáno ani není diskutováno jak velká část byla přebrána, jednotlivé komponenty nejsou popsány ani vysvětleny důvody, proč jsou použity.

5. Formální úprava technické zprávy **55 b. (E)**

Práce obsahuje velké množství drobných překlepů a nevhodných formulací. Občas je používán nespisovný jazyk a uměle vytvořená slova, např. str 14 jinačí cestou, retrénování modelu apod. Některé jazykové stylizace se nehodí do odborné práce.

6. Práce s literaturou **55 b. (E)**

Citace jsou v práci často shlukovány na koncích bloků textů, není na první pohled zřejmé, které části jsou odkud citovány. Většina práce obsahuje dostatečné množství referencí, ovšem u některých specifických oblastí chybí např. zcela chybí odkazy k polymorfnímu shellkódu, které mají být hlavním cílem práce.

7. Realizační výstup **65 b. (D)**

Aplikace je spustitelná a funkční. Úroveň zdrojového kódu je dobrá, dostatečně komentovaná. Výsledky testování jsou na první pohled zajímavé, opravdu odhalily slabiny testovacích IDS systémů. Testování ovšem nezohledňuje výsledky jiných aplikací podobného typu, takže není možnost srovnání. Dále na základě výsledků nejsou vyvozeny závěry jak jich využít.

8. Využitelnost výsledků

Využitelnost výsledků se mi těžko vyhodnocuje kvůli absenci srovnání jiných nástrojů. Aplikace má potenciál rozšířit množství nástrojů pro testovací účely.

9. Otázky k obhajobě

- Na základě jakých parametrů byly vybrány exploity a mutátotry?
- Odkud jsou převzaty principy mutátorů?

10. Souhrnné hodnocení **60 b. uspokojivě (D)**

Práce je poměrně nevyvážená. Velmi dobrou částí je část implementační kdy jak popis implementace tak realizovaný výstup je dobrý. Úroveň ovšem sráží velké množství nedokonalostí v jiných částech. Není jasná míra přispění studenta v návrhové části. Student dobře využívá kombinování základních stavební bloky řešení tak, aby vzniklá aplikace byla funkční, ovšem zcela chybí teorie k těmto stavebním blokům, např. vlastnosti mutace, které parametry zde hrají roli apod. Kvalita výsledného řešení pak není dobře podložena.

V Brně dne: 4. června 2015

.....
podpis