Posudek oponenta diplomové práce

Jméno diplomanta: Martin Čížek
Téma práce: Nasazení systému LaBrea6 do reálného provozu v síti IPv6

Diplomová práce se zabývá problematikou detekce útoků a monitorováním chování útočníka, k čemuž využívá systému LaBrea6 a honeypotů třetích stran.

V první části práce jsou popsány rozdíly mezi IPv4 a IPv6, které je třeba zohlednit při detekci chování útočníka. Následuje popis fungování systému LaBrea6, který diplomant vytvořil v rámci své bakalářské práce. Dále se práce zabývá problematikou a metodikou skenování adresního prostoru v IPv6, jejíž hlavní úskalí spočívá ve velikosti adresního prostoru, kdy není možné tuto akci provádět hrubou silou, ale je třeba použit sofistikovanější metody. Na základě tohoto popisu diplomant navrhl schéma adresního prostoru, který má u útočníka navodit pocit reálného stroje a přilákat tak jeho pozornost. Kromě samotného návrhu adresního prostoru jsou popsány i tři varianty honeypotů pro ssh, smtp a www služby.

Tato teoretická část se v nemalé míře překrývá s obsahem bakalářské práce diplomanta a některé části, například rozdíly IPv4 a IPv6 vypadají téměř převzatě. U obrázků, například 2.1 není uveden autor, ale v bakalářské práci jsou označeny jakou převzaté. U této části práce velmi postrádám hlubší teoretický základ, tedy pokud řešíme, bezpečnost zmínit zde důvody a cíle útoků, typy útoků, možnosti detekce a obrany, vysvětlení pojmů jako je IDS či honeypot a v případě honeypotů důvody pro sběr informací o chování útočníka. Zcela zde chybí představení již existujících řešení, jejich zhodnocení a důvody pro tvorbu systému nového.

V praktické části je nejprve velice stručně popsána implementace generátoru konfigurace a navrženého adresního prostoru. Následuje popis a problémy výše zmíněných honeypotů. Dále je pomocí screenshotů a stručného popisu představeno webové prostředí LaBrea6 a jeho jednotlivé části, včetně možnosti reportingu a mobilní klient pro přístup k nasbíraným datům.
V závěrečné části práce je zmíněn instalační skript pro celý systém a zhodnocení měsíčního provozu v laboratořích CIV, kde systém zaznamenal dva útoky.

Popis implementace je extrémně stručný, jsou zde pouze vyjmenovány zdrojové soubory pro generování adresního prostoru, ale například systém pro sběr a parsování logů, který se používá pro jednotlivé honeypoty není popsán vůbec. Stejně tak instalace systému LaBrea6 a jednotlivých honeypotů je velice stručná. Jednotlivé systémy jako například Kippo SSH nejsou zcela jistě prací diplomata ani běžnou součásti distribuce, ale kde je možné je získat pro následnou instalaci není nikde uvedeno. Zvláštní mi přijde fakt, že pro překlad systému LaBrea6 je třeba práv administrátora, ale pro instalaci součásti systému pomocí apt-get ne. U webového rozhraní zcela chybí jakékoliv zabezpečení či autorizace, což je u systému, který má shromažďovat informace o útočnících velmi zásadní chyba, neboť útočník pokud narazí na tento stroj snadno zjistí, že byl odhalen. Celý systém je prezentován jako systém pro IPv6 a je tak i navržen, ale vyjma definice adresního prostoru příliš nevidím co brání použití i pro IPv4 a proč nebyl systém od počátku koncipován jako hybridní, což by významně zvýšilo jeho použitelnost. K definici adresního prostoru mám také jednu výhradu, systém se snaží navodit pocit reálné sítě včetně služeb, ale vygenerovaná konfigurace je zcela plochá, což neodpovídá parametrům běžné sítě.

SOUHLASÍ
S ORIGINÁLEM

Kromě technických a formálních nedostatků, které jsou uvedené v předchozích odstavcích, obsahuje práce i různé překlepy. Celkově mám dojem, že student patrně odvedl více práce než kolik je uvedeno v textu, který působí nekompletně. Především teoretická část by potřebovala rozvést a doplnit. V praktické části bych uvítal přesnější popisy nasazení a konfigurace jednotlivých částí. Přínosné by bylo i jasnější rozdělení práce vykonané v rámci bakalářské a diplomové práce.
Na diplomanta mám následující dotazy:

- Co brání podpoře IPv4 v rámci odvedené práce ?
- Proč není implementován a jak složité by bylo v systému simulovat větší členitost adresního prostoru, tedy směrování požadavků přes více uzlů, místo plochého adresního prostoru?
- Je v rámci Kippo SSH možné zaznamenávat i neinteraktivní zadávání příkazů ?

I přes velké množství nedostatků práce splňuje zadání, na základě čehož ji doporučuji k obhajobě a hodnotím klasifikačním stupněm

Dobře

Ing. Luboš Matějka
KIV, ZČU Plzeň

V Plzni, 4.6.2013

Západočeská univerzita v Plzni
Fakulta aplikovaných věd
katedra informatiky a výpočetní techniky