Rozšírené zadanie diplomovej práce

Názov práce: Generovanie honeypotov na základe dôkazov zneužiteľnosti zraniteľností

Autor práce: Bc. Filip Dvorský

Vedúci práce: RNDr. Tomáš Bajtoš, PhD.

Ciele práce:

1. Zmapovať aktuálne prístupu ku generovaniu honeypotov.
2. Navrhnúť a implementovať systém na generovanie honeypotov na základe dôkazov zneužiteľnosti zraniteľností.
3. Overenie funkčnosti riešenia pomocou simulovaných útokov na zvolené zraniteľnosti.

Popis:

Nové technológie so sebou prinášajú nové typy útokov a kybernetických hrozieb, ktoré si vyžadujú nové flexibilné prístupy a nástroje k monitorovaniu a prevencii daných hrozieb. Jedným z týchto kľúčových nástrojov sú aj Honepoty. Honepoty sú zariadenia určené ako pasce na útočníkov, snažiacich sa získať prístup k zariadeniu, získať dáta z daného zariadenia atď., pričom honepot počas útoku monitoruje aktivitu útočníka, čo následne pomáha zlepšovať bezpečnostné opatrenia ako napríklad nastavenie firewall-u, Threat-Hunting a mnoho ďalších.

Tradičné honeypoty však čelia výzvam, ako je napríklad neschopnosť reagovať na nové zraniteľnosti v reálnom čase, ale aj generovanie veľkého množstva údajov a dát, z ktorých podstatná časť má nízku výpovednú hodnotu pre bezpečnostného analytika. Tradičným príkladom sú tzv. “script kiddies“, sú to útočníci, ktorí využívajú základné nástroje na vykonávanie jednoduchých automatizovaných útokov. Výsledkom je teda zahltenie

bezpečnostného analytika nepotrebnými informáciami, čo vo výsledku komplikuje a predlžuje prácu analytika.

Jednotlivé dôkazy zneužiteľnosti zraniteľností sú zväčša písane v programovacích jazykoch Ruby a Python. Zväčša tieto dôkazy spúšťajú nejaké neškodné zabudované programy ako napríklad kalkulačka alebo vypíšu nejaký špecifický reťazec ako demonštráciu funkčnosti danej zraniteľnosti na zariadení.

```
try:
    response = requests.post(target + path, headers=headers, json=create_element(nonce), verify=False, timeout=10)
    response.raise_for_status()
    if response.status_code == 200 and 'KHABuhwxnUHDDW' in response.text:
        color.print(f"[bold bright_green][+][/bold bright_green] Identified vulnerability in target: [bold cyan]{target}[/bold cyan]"
        break
```

Obrázok č. 1: Ukážka časti dôkazu zneužiteľnosti zraniteľností CVE-2024-25600

Na obr. č. 1 môžeme vidieť ukážku z dôkazu zneužiteľnosti zraniteľností CVE-2024-25600 napísanú v jazyku Python, ktorá umožňuje vzdialené spustenie kódu na službe Wordpress pri použití témy “Bricks”. Daný kód vytvorí požiadavku a očakáva odpoveď zo špecifickým reťazcom, v tomto prípade reťazec “KHABuhwxnUHDDW”. Keďže požiadavka má určitú štruktúru a daný reťazec bol predom špecifikovaný, vieme vytvoriť nízko úrovňový honeypot, ktorý bude simulovať reálny systém.

Hlavným cieľom tejto práce je navrhnúť, implementovať a overiť systém, ktorý bude pomocou dôkazu zneužiteľnosti zraniteľností vytvárať honeypot pre daný dôkaz zneužiteľnosti zraniteľností. Pričom naše zameranie bude na dôkazy zneužiteľnosti zraniteľností pre služby fungujúce na protokole HTTPS a HTTP a teda na portoch 443 a 80.

Práca sa zameria na tri hlavné ciele:

1. **Zmapovanie aktuálnych prístupov ku generovaniu honeypotov:**

   V tejto časti preskúmame jednotlivé prístupy na generovanie honepotov (rule-based prístup, atď.), spolu so získaním a vytriedením dôkazov zneužiteľnosti zraniteľnosti. Taktiež dane dôkazy rozdelíme do jednotlivých skupín v závislosti od služby, ktorá bude zasiahnutá a samotnej zložitosti dôkazu.

2. **Návrh a implementácia systému:**

   Návrh a implementácia systému na generovanie honeypotov bude závisieť od početnosti dôkazov zneužiteľnosti zraniteľností. Pričom pri návrhu a implementácii sa budeme zameriavať na Rule-based prístup a teda náš systém, podľa určitých pravidiel nájde špecifické časti v danom dôkaze, napr. špecifické reťazce na výstupe, a podľa týchto pravidiel vytvorí honeypot, ktorý bude simulovať danú zraniteľnú službu.

3. **Overenie funkčnosti riešenia:**

   Funkčnosť riešenia budeme overovať simulovanými útokmi na nami vybrané zraniteľnosti. Cieľom bude analyzovať efektívnosť generovaných honeypotov pri získavanie údajov z útokov.

Literatúra:

1. MUSCH, Marius; HÄRTERICH, Martin; JOHNS, Martin. Towards an automatic generation of low-interaction web application honeypots. In: Proceedings of the 13th international conference on availability, reliability and security. 2018. p. 1-6.
2. SPITZNER, Lance. Honeypots: Catching the insider threat. In: 19th Annual Computer Security Applications Conference, 2003. Proceedings. IEEE, 2003. p. 170-179.
3. SPITZNER, Lance, et al. Know your enemy. Addison-Wesley, 2002.