Detekcia honeypotov

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

Honeypot

- mechanizmus, ktorého hlavným účelom je monitorovať neautorizovaný prístup k informačným systémom
- sleduje aktivitu útočníka
- podľa definície honeypot vidí iba „zlú“ aktivitu, nezachytáva bežnú činnosť
- 2 alebo viac honeypotov v sieti tvorí honeynet

- detekcia honeypotov – dôležitá kvôli zvýšeniu ich efektívnosti

Aktuálne prístupy

- detekcia je rôzna v závislosti od typu honeypotu
  - **nízko až stredne interaktívne honeypoty**
  - identifikácia na úrovni siete, aplikácií, služieb
  - **vysoko interaktívne honeypoty**
  - identifikácia na úrovni systému, operačná analýza

Detekcia honeypotov v súčasnosti

výber konkrétneho honeypotu

↓

metóda detekcie

↓

popis metódy

Honeyd

↓

testovanie služby, ktorú predstavuje

↓

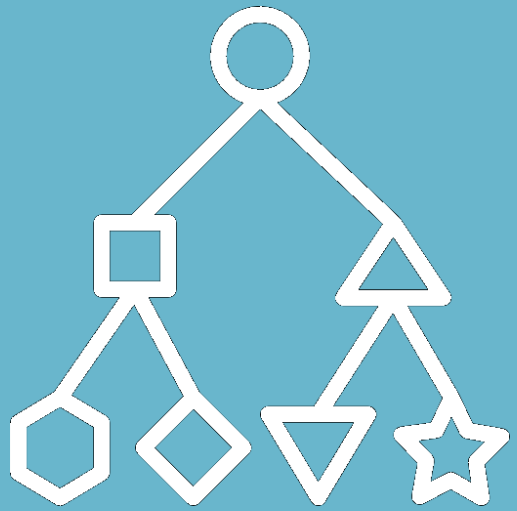
TCP/IP fingerprinting

Detekcia honeypotov v súčasnosti

Service	Feature / command	Real systems	Honeyd
HTTP	GET	✓	✓
	OPTINOS	✓	×
	HEAD	✓	×
	TRACE	✓	×
FTP	USER	✓	✓
	PASS	✓	✓
	MODE	✓	×
	RETR	✓	×
SMTP	HELO	✓	✓
	MAIL	✓	✓
	DATA	✓	×
	VRFY	✓	×
	ETRN	✓	×

Detekcia honeypotov vo všeobecnosti

- klasifikácia honeypotov do všeobecných skupín
- delenie honeypotov
  - podľa interaktivity
  - aktívny – pasívny
  - fyzický – virtuálny
  - server – klient
  - ...



Podvodné systémy

- 6 základných kategórií podvodu:
  masking, repackaging, dazzling, mimicking, inventing, decoying
- typ honeypotu reflektuje spôsob jeho maskovania

- napríklad ak je honeypot zaradený ku typu podvodu, ktorý využíva návnadu – budeme v systéme hľadať podvrhnuté heslá, súbory,...

Najčastejšie využívané kategórie?

- zoznam dostupných honeypotov (typ, udržiavanosť, účel, jazyk, typ databázy)

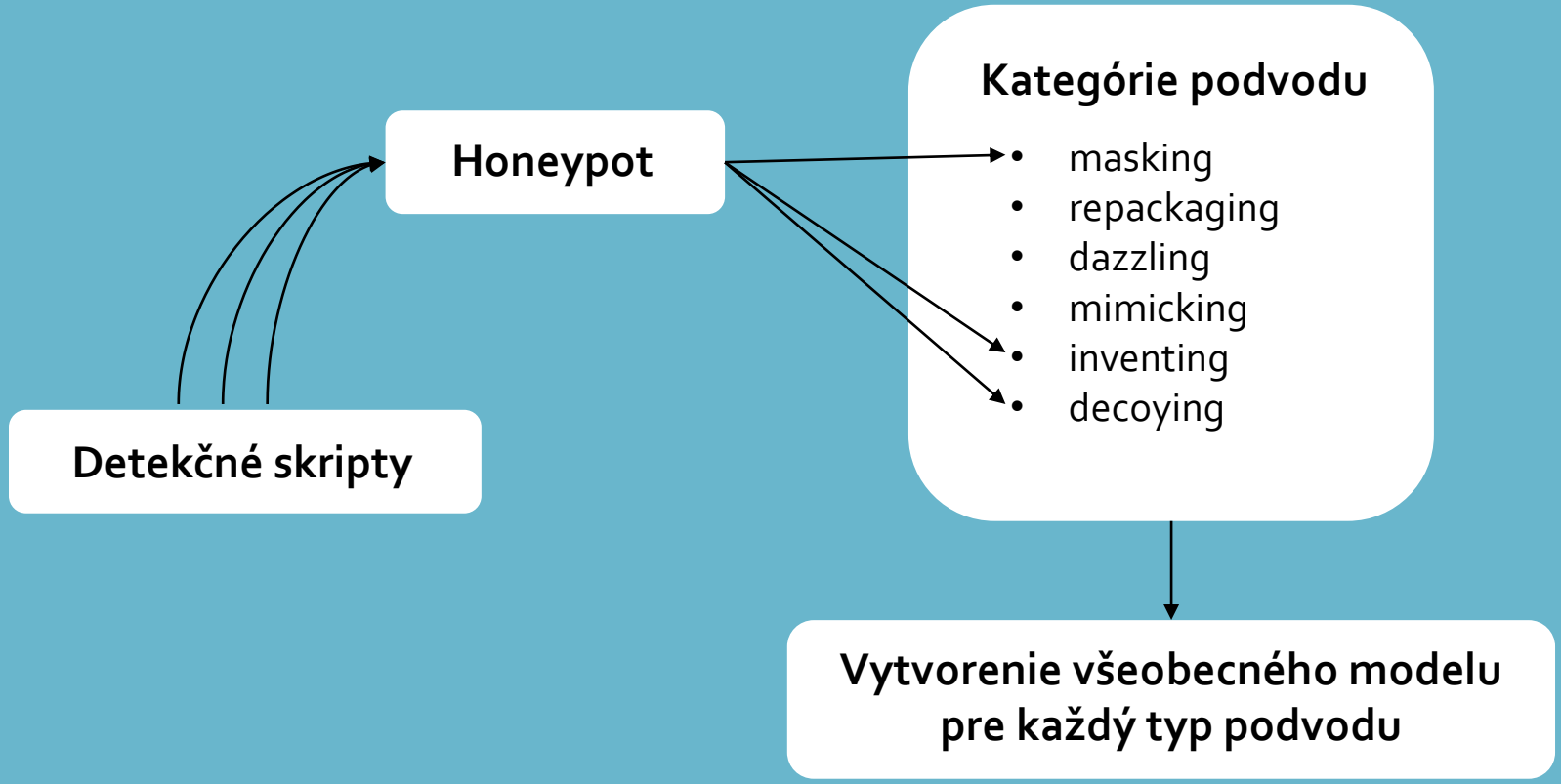
- **serverové honeypoty** (Kippo, Dionaea)
- **webové honeypoty** (Glastopf)
- **SSH, telnet, IoT,...**

Detekcia pomocou Pythonu

- jednoduché ale aj zložitejšie skripty založené na rôznych vlastnostiach konkrétnych honeypotov
- detekcia vybraných honeypotov
- hlbšie pochopenie toho ako daný honeypot pracuje
- zaradenie honeypotu do konkrétnej kategórie podvodu
- vytvorenie modelu pre každú kategóriu podvodu

- *ukážka...*

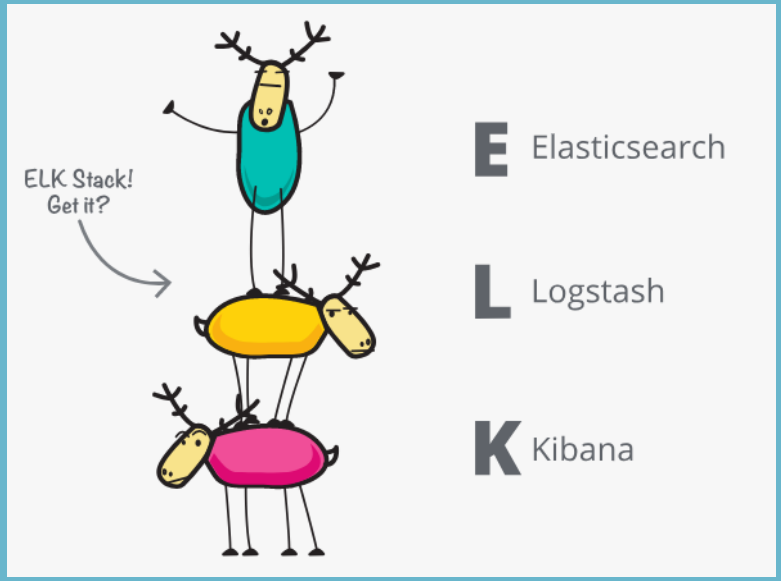
Štruktúra práce



Vyhodnotenie nástroja: T-Pot

- kolekcia honeypotov zostavená spoločnosťou T-Mobile

- adbhoney
- ciscoasa
- conpot
- cowrie
- dionaea
- elasticpot
- glastopf
- glutton
- heralding
- honeypy
- honeytrap
- mailoney
- medpot
- rdpy
- snare
- tanner



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

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 Survey on 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.

Ďakujem za pozornosť