
# Detekcia honeypotov

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

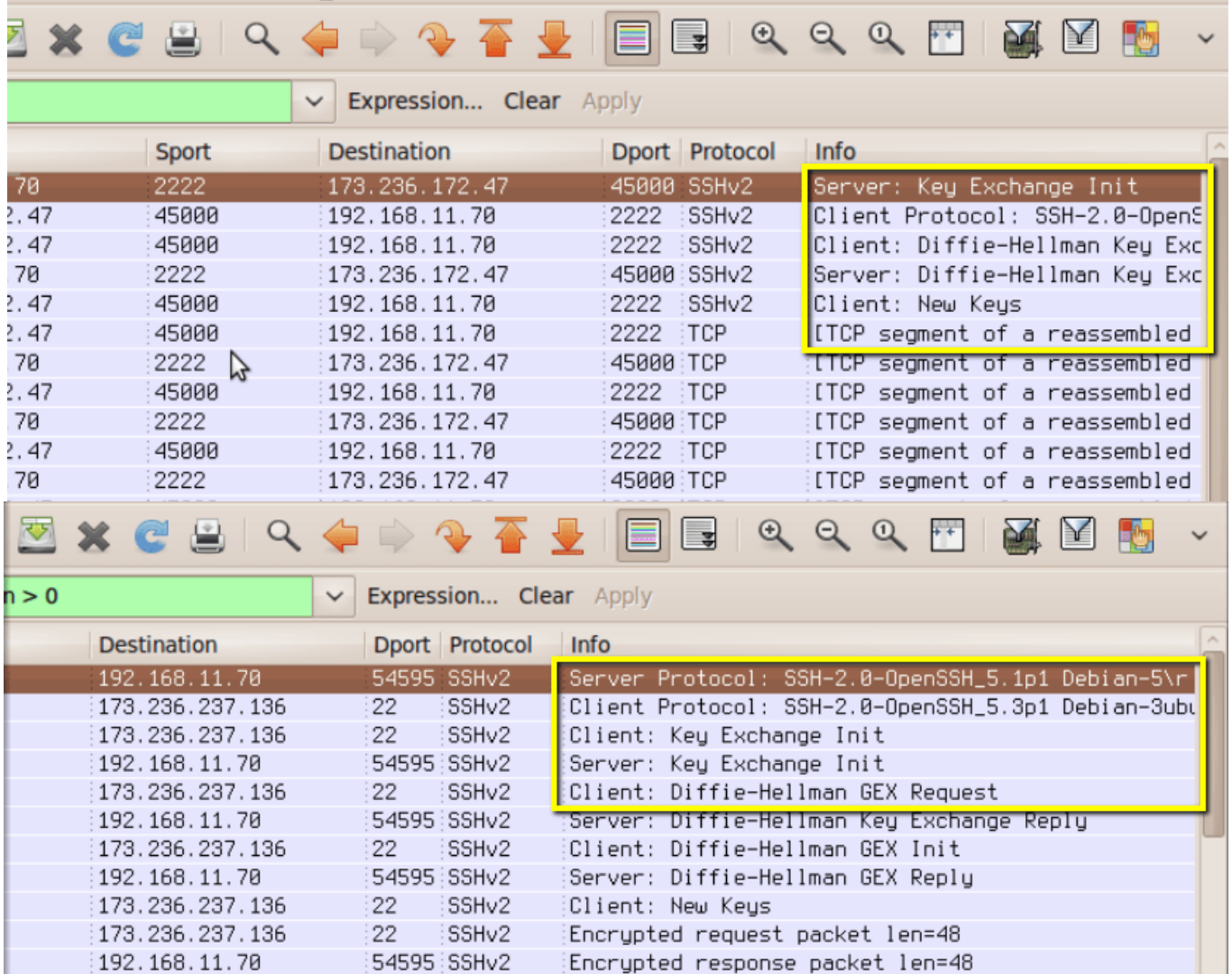
# Motivácia

- 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


Expression... Clear Apply
Sport Destination Dport Protocol Info
70 2222 173.236.172.47 45000 SSHv2 Server: Key Exchange Init
2.47 45000 192.168.11.70 2222 SSHv2 Client Protocol: SSH-2.0-OpenS
2.47 45000 192.168.11.70 2222 SSHv2 Client: Diffie-Hellman Key Exc
70 2222 173.236.172.47 45000 SSHv2 Server: Diffie-Hellman Key Exc
2.47 45000 192.168.11.70 2222 SSHv2 Client: New Keys
2.47 45000 192.168.11.70 2222 TCP [TCP segment of a reassembled
70 2222 173.236.172.47 45000 TCP [TCP segment of a reassembled
2.47 45000 192.168.11.70 2222 TCP [TCP segment of a reassembled
70 2222 173.236.172.47 45000 TCP [TCP segment of a reassembled
2.47 45000 192.168.11.70 2222 TCP [TCP segment of a reassembled
70 2222 173.236.172.47 45000 TCP [TCP segment of a reassembled
n > 0 Expression... Clear Apply
Destination Dport Protocol Info
192.168.11.70 54595 SSHv2 Server Protocol: SSH-2.0-OpenSSH_5.1p1 Debian-5\r
173.236.237.136 22 SSHv2 Client Protocol: SSH-2.0-OpenSSH_5.3p1 Debian-3ubu
173.236.237.136 22 SSHv2 Client: Key Exchange Init
192.168.11.70 54595 SSHv2 Server: Key Exchange Init
173.236.237.136 22 SSHv2 Client: Diffie-Hellman GEX Request
192.168.11.70 54595 SSHv2 Server: Diffie-Hellman Key Exchange Reply
173.236.237.136 22 SSHv2 Client: Diffie-Hellman GEX Init
192.168.11.70 54595 SSHv2 Server: Diffie-Hellman GEX Reply
173.236.237.136 22 SSHv2 Client: New Keys
173.236.237.136 22 SSHv2 Encrypted request packet len=48
192.168.11.70 54595 SSHv2 Encrypted response packet len=48

# 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.

# Zdroje


- www.honeypot.io
- www.honeynet.org
- M. Dornseif ; T. Holz ; C.N. Klein: NoSEBrEaK - attacking honeynets
- A. Vetterl; R. Clayton: Systematically Fingerprinting Low- and Medium-interaction Honeypots at Internet Scale
- J. Uitto; S. Rauti; S. Laurén; V. Leppänen: A Survey on Anti-honeypot and Anti-introspection Methods

# Ďakujem za pozornosť