# Identifikácia fáz útoku v počítačovej sieti

Bc. Marek Dorko

Vedúci práce: RNDr. JUDr. Pavol Sokol, PhD.

Konzultant: RNDr. Tomáš Bajtoš

ÚINF

2. 12. 2022

# Motivácia

- útoky sa stali zložitejšími
- niekoľko krokov na dosiahnutie svojho cieľa

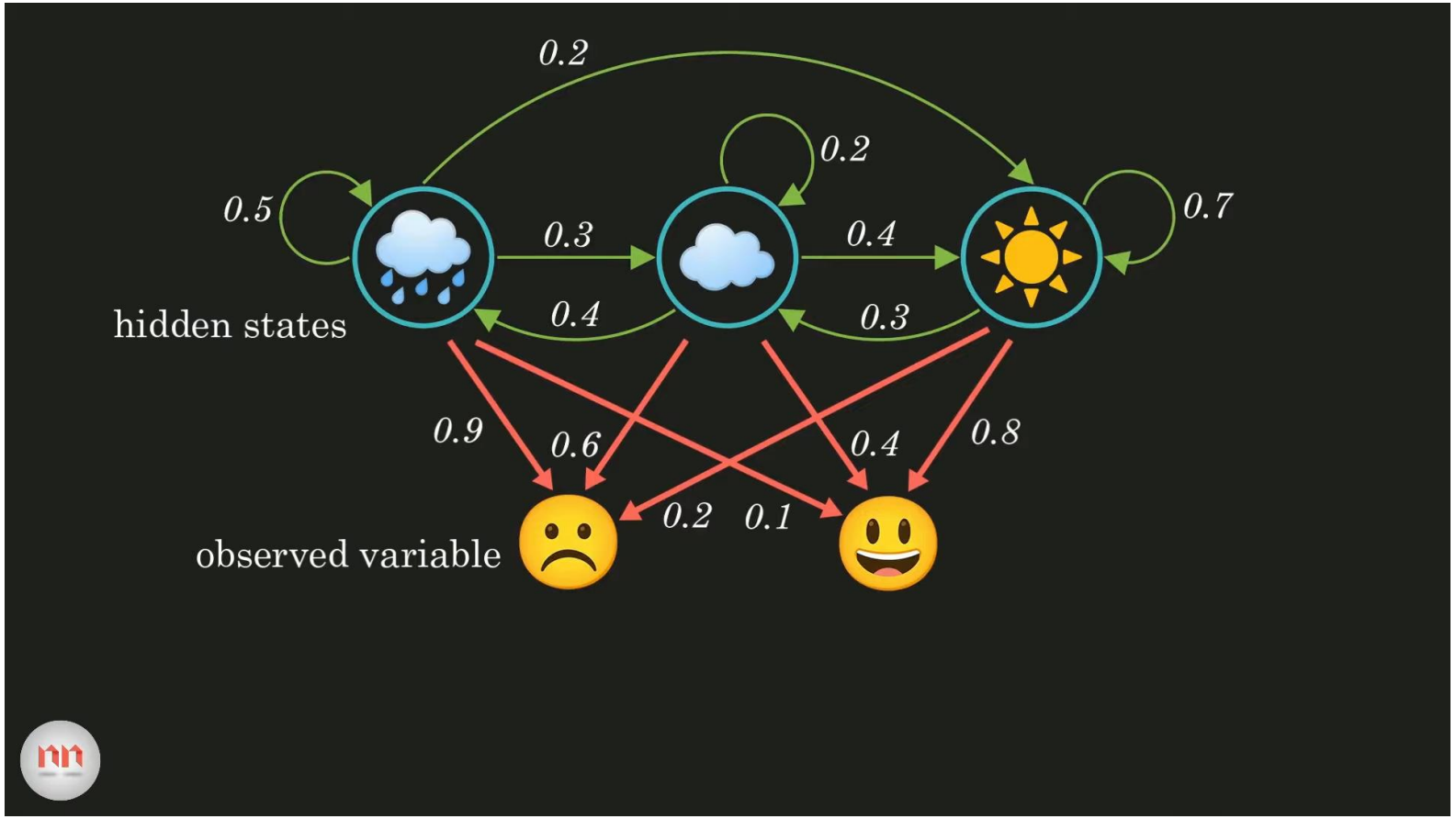
# Ciele práce

1. Analyzovať prístupy k identifikácii fáz útoku v počítačovej sieti.
2. Porovnať prístupy k identifikácii fáz útoku v počítačovej sieti pomocou digitálnych stôp z koncových zariadení.
3. Navrhnúť a implementovať model identifikácie fáz útoku v počítačovej sieti, vyhodnotenie efektívnosti tohto modelu.

# Postup pri riešení

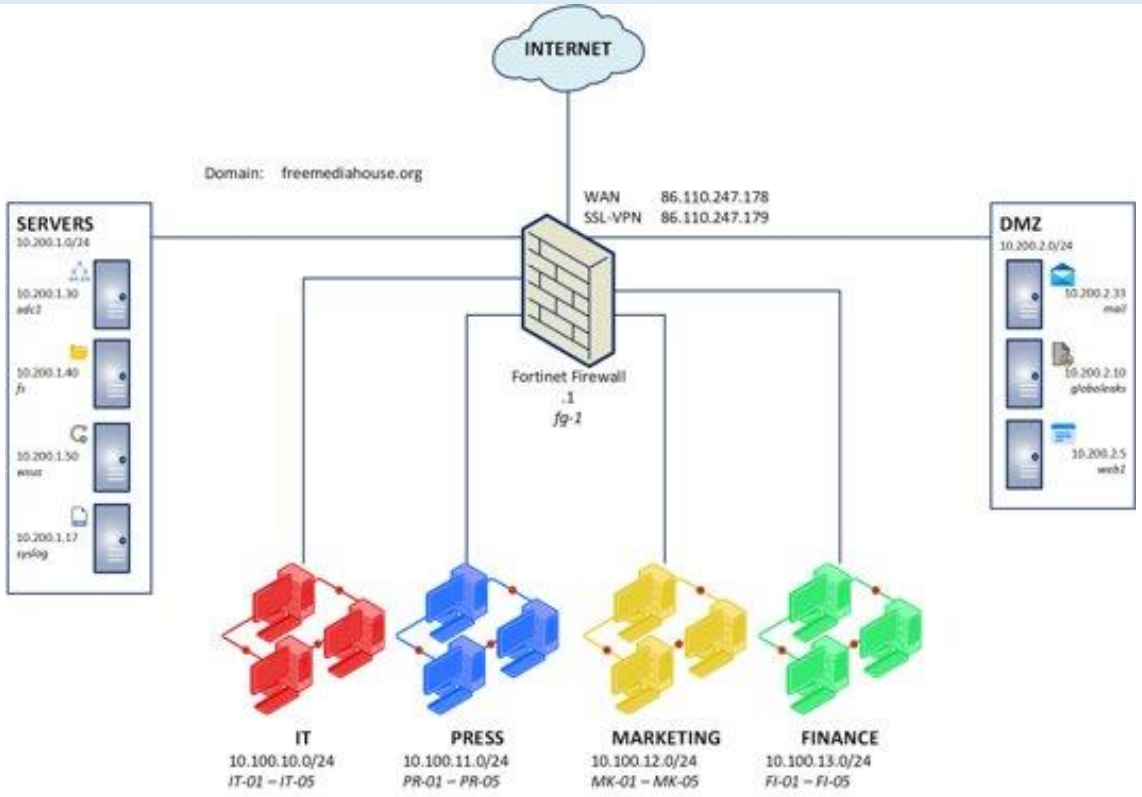
- preštudovanie podobných prác
- oboznámenie sa s datasetom
- vhodný model – Hidden Markov Model

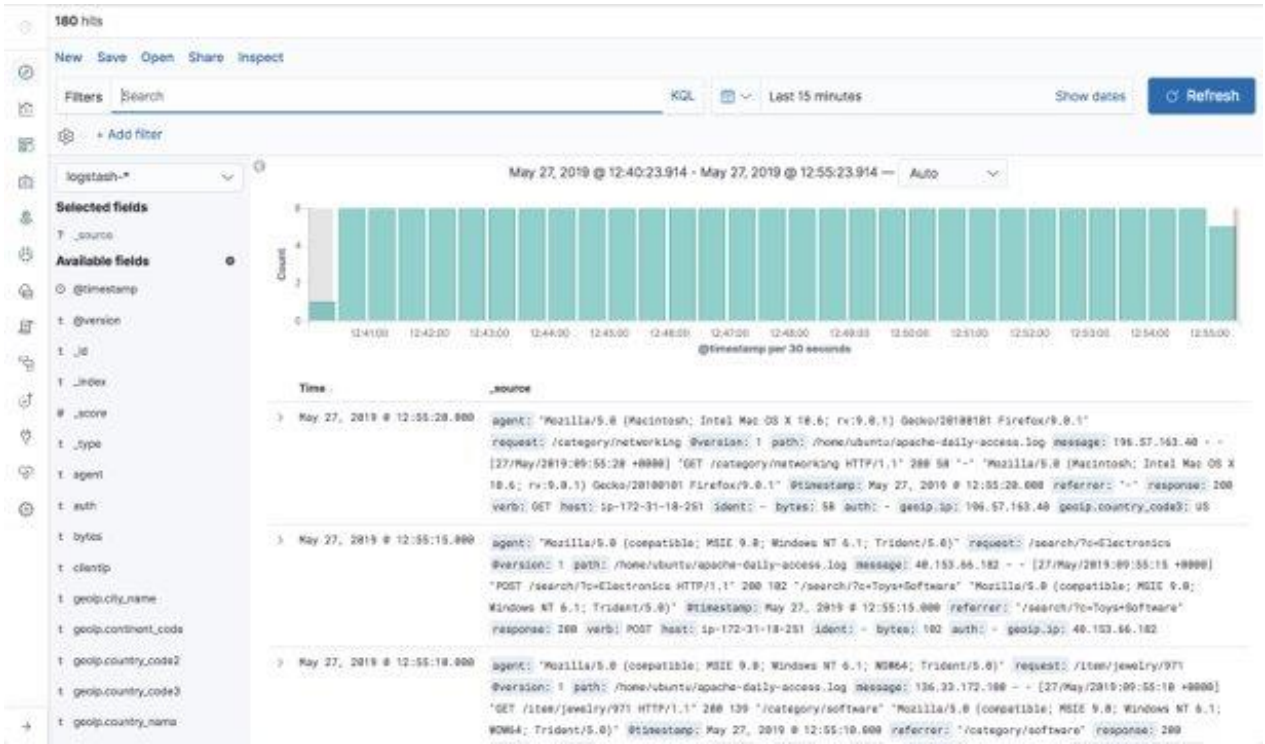
# Hidden Markov Model




Zdroj: https://www.youtube.com/@NormalizedNerd

# Dataset


INTERNET
Domain: freemediahouse.org
WAN 86.110.247.178
SSL-VPN 86.110.247.179
SERVERS
10.200.1.0/24
10.200.1.30
adc1
10.200.1.40
fs
10.200.1.50
wsus
10.200.1.17
syslog
Fortinet Firewall
.1
fg-1
DMZ
10.200.2.0/24
10.200.2.33
mail
10.200.2.10
globaleaks
10.200.2.5
web2
IT
10.100.10.0/24
IT-01 – IT-05
PRESS
10.100.11.0/24
PR-01 – PR-05
MARKETING
10.100.12.0/24
MK-01 – MK-05
FINANCE
10.100.13.0/24
FI-01 – FI-05


160 hits
New Save Open Share Inspect
Filters Search KQL Last 15 minutes Show dates Refresh
+ Add filter
logstash-*
May 27, 2019 @ 12:40:23.914 - May 27, 2019 @ 12:55:23.914 — Auto
Selected fields
_source
Available fields
@timestamp
@version
_id
_index
_score
_type
agent
auth
bytes
clientip
geoip.city_name
geoip.continent_code
geoip.country_code2
geoip.country_code3
geoip.country_name
Count
@timestamp per 30 seconds
Time
_source

# Literatúra


1. Navarro, J., Deruyver, A., & Parrend, P. (2018). A systematic survey on multi-step attack detection. Computers & Security, 76, 214-249.
2. Aparicio-Navarro, F. J., Kyriakopoulos, K. G., Ghafir, I., Lambotharan, S., & Chambers, J. A. (2018, October). Multi-stage attack detection using contextual information. In MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM) (pp. 1-9). IEEE.
3. Takey, Y. S., Tatikayala, S. G., Samavedam, S. S., Eswari, P. L., & Patil, M. U. (2021, March). Real Time early Multi Stage Attack Detection. In 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 283-290). IEEE.
4. Wilkens, F., Ortmann, F., Haas, S., Vallentin, M., & Fischer, M. (2021, November). Multi-Stage Attack Detection via Kill Chain State Machines. In Proceedings of the 3rd Workshop on Cyber-Security Arms Race (pp. 13-24).
5. CHADZA, Timothy; KYRIAKOPOULOS, Konstantinos G.; LAMBOTHARAN, Sangarapillai. Analysis of hidden Markov model learning algorithms for the detection and prediction of multi-stage network attacks. *Future generation computer systems*, 2020, 108: 636-649.
6. GHAFIR, Ibrahim, et al. Hidden Markov models and alert correlations for the prediction of advanced persistent threats. *IEEE Access*, 2019, 7: 99508-99520.
7. ZHANG, Xu, et al. Multi-Step Attack Detection Based on Pre-Trained Hidden Markov Models. *Sensors*, 2022, 22.8: 2874.

Ďakujem za pozornosť.